ZRÍNYI MIKLÓS
NEMZETVÉDELMI EGYETEM

Muha Lajos

A MAGYAR KÖZTÁRSASÁG KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁINAK VÉDELME

Doktori (PhD) értekezés

Tudományos vezető:

Dr. Kovács László mérnök őrnagy, PhD
egyetemi docens

Budapest, 2007.

TARTALOMJEGYZÉK

> *„Egy kibertámadás esélye és veszélye napról napra nő, és mi gyakorlatilag semmit sem teszünk ez ellen… A terroristák, legyen az a Hamász, vagy az al-Kaida, képesek hozzáférést szerezni az erőműveinkhez, a légiforgalmi irányítási rendszereinkhez, a közműveinkhez és a bankrendszereinkhez, ami sötétségbe borít, elnémítja a telefonvonalakat, és kitörli a bankszámlákat. Egyes szakértők egy digitális Pearl Harbor-ként írják le nekünk ezt a valós sebezhetőséget … én félek, hogy egy digitális Armageddon határán vagyunk."* [94]

BEVEZETÉS

A modern társadalmak nagymértékben függenek az infrastruktúráktól (energiaellátás, ivóvízellátás, kommunikációs rendszerek és informatikai hálózatok stb.), amelyek komplex rendszerét az egymástól való függőségek jellemzik. A közelmúltban bekövetkezett terrortámadások (New York WTC, Madrid, London), természeti katasztrófák (ázsiai szökőár, földrengések) és technikai kihívások (kétezredik évi dátumváltás, nagykiterjedésű áramkimaradások, kibertámadások) felhívták a figyelmet az infrastruktúrák sebezhetőségére, valamint az infrastruktúrák, a társadalom és kormányzati működés kölcsönös egymásrautaltságára. E rendszerek működési zavarai, illetve egyes elemeinek ideiglenes kiesése, vagy megsemmisülése jelentős kihatással vannak mindennapi életünkre, a közigazgatás, a gazdaság hatékony működésére, a lakosság életére. Elvárható a kritikus infrastruktúrák elemei terrorcselekményekkel, természeti katasztrófákkal és balesetekkel szembeni védelme érdekében, hogy az infrastruktúrák működésének megzavarása vagy manipulálása megelőzhető, kivédhető, illetve a lehetséges mértékben rövid, kivételes és kezelhető legyen. Más szóval, nem csak az állam, a gazdaság szereplői, de az egész társadalom részéről elvárás, hogy e kritikus infrastruktúrák a lehető legnagyobb biztonsággal működjenek.

A modern állam, annak minden szervezete és polgára kiszolgáltatottá vált a számítógépekből, kommunikációs eszközökből és automata rendszerekből álló bonyolult, többszörösen összetett információs infrastruktúrának. Napjainkban ezen eszközök nélkül életünk elképzelhetetlenné vált. Vezetékes és mobil telefonon tartjuk szeretteinkkel a kapcsolatot, ha pénzre van szükségünk a bankjegykiadó automatához (ATM) fordulunk, amelynek a lényege egy személyi számítógép, ami vezetékes telefonvonalon keresztül a bankunk vagy az elszámoló központ számítógépére csatlakozik, és digitális kommunikációjuk dönti el, hogy kaphatunk-e készpénzt az automatából vagy sem. Munkahelyünkön a

munkánkhoz szükséges adatok jelentős része a számítógépen van tárolva. A legtöbb esetben már nem is a saját asztali számítógépünkön, hanem távol, néha több száz vagy ezer kilométerre lévő központi számítógépeken. Ezek a számítógépeken tárolt adatok teszik lehetővé, hogy például a villamosenergia-szolgáltatónk átlássa, hol mennyi áramra van szükség, és honnét tudja azt beszerezni. Ha ezekben a rendszerekben bárhol, bármilyen hiba adódik, máris elindul egy dominóhatás. Villamos energia nélkül más számítógépek is leállnak, sötétség lesz, de még hideg is, mert az elektromosan vezérelt gázfűtésünk is leáll. Ha nem működnek a bankjegykiadó automaták, akkor még a vésztartalék petróleumlámpával világító üzletben sem tudjuk alapvető létszükségleti cikkeinket beszerezni. Ez olyan káoszba torkollhat, amelynek kimenetele nehezen jósolható meg.

Tudomásul kell vennünk, hogy információs rendszereink és hálózataink egyre gyakrabban szembesülnek az igen sokféle forrásból származó biztonsági fenyegetéssel, többek között gazdasági hírszerzéssel, ipari kémkedéssel, számítógépes csalással, szabotázzsal, vandalizmussal, tűzzel vagy árvízzel. A szándékos károkozások olyan formái, mint a számítógépvírusok, a számítógépes betörések, vagy a szolgáltatás megtagadásra vezető támadások egyre gyakoribbá, általánosabbá válnak, ugyanakkor ezek egyre vakmerőbbek és egyre bonyolultabbak is. Egyre nagyobb fenyegetést jelent sérülékeny információs rendszereinkre a hadviselés új formája az információs hadviselés, de még inkább a békeidőkben is állandóan fenyegető terrorizmus számítógépes változata, a kiberterrorizmus.

A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

Veszélyben vannak az infrastruktúráink, azok közül is elsősorban azok, amelyek működése **elengedhetetlen** a gazdaság és a társadalom **zavartalan működéséhez**. A különböző infrastruktúrák, eszközök, és szolgáltatások bármelyikének megsemmisülése vagy sérülése a társadalom széles rétegeit érinti. A modern gazdasági berendezkedés mellett a társadalom nincs felkészülve arra, hogy a kiesett infrastruktúrák, eszközök vagy szolgáltatások nélkül működjön, így ezeket – egyértelműen – védeni kell. A világban mintegy tíz éve megkezdődött ezeknek, az egyes országoknak a szempontjából kritikus infrastruktúráknak a szervezett, összehangolt és többnyire tudományosan is alátámasztott védelme.

Már a kezdetektől sokan belátták, hogy napjainkban az információs rendszerek nélkülözhetetlenné váltak a társadalom egésze számára, mert az állam működése, a különböző szolgáltatások megvalósítása és igénybevétele elképzelhetetlen ezek nélkül a rendszerek

nélkül. Már önmagukban ezeknek az információs rendszereknek a kiesése is katasztrófahelyzetet idézhet elő.

A különböző infrastruktúrák, eszközök és szolgáltatások túlnyomó többségének működése az információs rendszereken alapszik. Az infrastruktúrák belső információs rendszerének megsemmisülése vagy sérülése az egész infrastruktúrát megbéníthatja, sőt az infrastruktúrák kölcsönös függősége, egymásra utaltsága miatt az egyik infrastruktúra belső információs rendszerének a sérülése a másik infrastruktúra működési zavarait okozhatja.

Az információs infrastruktúrák, az információs rendszerek nem csak a fizikai veszélyeknek vannak kitéve, hanem más, a kibertérből érkező támadásokkal szemben is nehezen védhetők. Az információs rendszerek támadásával – azaz a kritikus információs infrastruktúrák működésének időleges vagy teljes működésképtelenségével – az infrastruktúráink nagy része megbénítható. Egy jól megválasztott támadás, amely egy infokommunikációs rendszer ellen irányul akár az egész ország, vagy akár egy szubregionális infokommunikációs rendszer sérüléséhez, vagy akár teljes leálláshoz vezethet. Mivel a gazdasági élet szereplői – a termelő vállalatok, a kereskedelem, a tőzsde, stb. – napi működéséhez sok esetben elengedhetetlenek egyes infokommunikációs rendszerek, ezért ezek támadásával, időszakos bénításával, működésképtelenné tételével, vagy akár végleges kiiktatásával igen nagy anyagi károk is előidézhetők. [47] Ezt a problémát felismerve a kritikus infrastruktúrák védelmén belül megjelent egy más megközelítést igénylő védelmi feladat, a kritikus információs infrastruktúrák védelme.

Hazánkban a kritikus információs infrastruktúrák védelme sajátos helyzetben van. Szövetségi rendszereink, az Európai Unió és a NATO ma már cselekvési egységben, a védelem összehangolásában gondolkodik, és ez kényszerítően visszahat a magyar biztonságpolitikára is. Hazánknak bizonyos lépéseket meg kell tennie, a szövetségi együttműködésből nem vonhatjuk ki magunkat.

Ugyanakkor nem történt még meg számos fogalom tisztázása, nem lettek egyértelműen kijelölve még a kritikus infrastruktúrák sem. Tisztázatlanok az állami, a gazdasági és a társadalmi feladatok, és ennek következtében a felelősök sincsenek kijelölve.

A kritikus információs infrastruktúráinkat fenyegető veszélyek feltárása, illetve az ellenük való védekezés módszereinek és eljárásainak kidolgozása tudományos kutatást igényel, amelyet – az elmúlt években az információs rendszerek védelme területén szerzett gyakorlati tapasztalataimra is támaszkodva – jelen doktori értekezésemben bemutatok.

KUTATÁSI HIPOTÉZISEK MEGFOGALMAZÁSA

1. A kritikus információs infrastruktúrák védelme állami feladat, ugyanakkor az üzleti, civil és akadémiai szféra széleskörű bevonását is igényli állami koordinációval.
2. A vonatkozó jogszabályok, szabványok, ajánlások megteremtése, illetve aktualizálása alapvető követelmény a kritikus információs infrastruktúrák védelme érdekében.
3. Az információbiztonsági tudatosság és az ismeretek széles körű fejlesztése nélkülözhetetlen a kritikus információs infrastruktúrák védelmében.
4. A kritikus információs infrastruktúrák védelméhez elsődleges állami feladat a folyamatos monitorozás, és a reagálási képesség megteremtése.

KUTATÁSI CÉLKITŰZÉSEK

Kutatásom során az alábbi célokat tűztem ki:

1. Nemzetközi tapasztalatok – különös tekintettel szövetségi rendszereinkre, a NATO-ra és az Európai Unióra – felhasználásával és azok hazai viszonyokra adaptálásával **meghatározni a kritikus infrastruktúra és kritikus információs infrastruktúra hazai fogalmát, tartalmát és elemeit.**
2. **Feltárni** a kritikus információs infrastruktúrákat fenyegető veszélyeket, **elemezni** a veszélyekre adható válaszokat – védelmi módszereket és eljárásokat –, valamint a meglévő nemzetközi jogszabályok, szabványok, ajánlások alkalmazhatóságát és teljesülését.
3. **Feltárni** a hazai kritikus információs infrastruktúrák védelmi helyzetét, a meglévő jogszabályok, ajánlások teljesülését, és e vizsgálat eredménye alapján **meghatározni a Magyar Köztársaság kritikus információs infrastruktúrák védelmének elsődleges feladatait.**
4. A hazai kritikus információs infrastruktúrák védelmének egyik meghatározó területeként **javaslatot tenni a Magyar Köztársaság infokommunikációs biztonsági stratégiájára**.

KUTATÁSI MÓDSZEREK

Kutatásaim kezdetén széleskörű irodalomkutatásra épülő **információk és adatok összegyűjtésével valamint rendszerezésével** összegeztem a különböző fejlett infrastruktúrával rendelkező országok, majd a NATO és az Európai Unió vonatkozó elvárásait, törekvéseit. A nemzetközi tapasztalatok elemzése alapján behatároltam a releváns hazai közigazgatási, gazdasági és társadalmi környezetet, azok elvárásait a kritikus információs infrastruktúrák védelmére. Mindeközben felhasználtam a **megfigyelést** és a **kritikai adaptációt**, majd számos kutatás és tanulmány **másodelemzésével**, az összefüggéseknek az **analízis** és **szintézis**, az **indukció** és **dedukció** módszereinek alkalmazásával törekedtem a kutatási céljaim elérésére és megvalósítására.

Mindezek alapján kutatásaimat a következő szerkezetű munkában foglalom össze:

Az első fejezetben meghatározom a kritikus infrastruktúra, a kritikus információs infrastruktúra magyar fogalmát és tartalmát.

A második fejezetben feltárom a kritikus információs infrastruktúrák védelmének nemzetközi gyakorlatát.

A harmadik fejezetben megvizsgálom a kritikus információs infrastruktúrák védelmének hazai megvalósítását, és ajánlást dolgozok ki a Magyar Köztársaság kritikus információs infrastruktúrák védelmére az általam feltárt hiányos, vagy rosszul működő területeken.

A dolgozatban az áttekinthetőség kedvéért *dőlt betű*kkel írom az *idézeteket*, a különböző *hivatkozott művek címei*t, valamint egyes *kiemelt szakkifejezéseket* első leírásukkor, **félkövér betű**kkel írom a **kiemelendő**, **fontos**nak tartott szavakat, kifejezéseket.

1. FEJEZET
KRITIKUS INFRASTRUKTÚRÁK ÉS KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK

Az irodalom a kritikus információs infrastruktúrák tekintetében sokrétű. A témára nagyon részletes és átfogó kitekintést ad a svájci Szövetségi Technológiai Intézet Biztonsági Tanulmányok Központjának kiadványa az *International CIIP Handbook 2006* [56], amely két kötetben összesen 733 oldalon tárgyalja e témát és feldolgozza 20 ország, 6 nemzetközi szervezet kritikus információs infrastruktúrával kapcsolatos rendelkezéseit, elképzeléseit, bemutatja az állami és civil szféra ezzel kapcsolatos intézkedéseit, továbbá koncepciókat és elemzéseket ismertet a témában. Már önmagában is érdemes e vaskos kézikönyvre támaszkodni[1], de a kutatás elfogulatlanságára és minél teljesebbé tétele érdekében más irodalmakat is feldolgoztam.

Magyarországon, az Európai Unió és a NATO tagjaként, elsődlegesen a szövetségi rendszerek elvárásait, meghatározásait kell figyelembe venni, de szövetségi rendszereink, környezetünk más államai gyakorlatának vizsgálata sem elhanyagolható. Az *International CIIP Handbook 2006* [56] első kötete első fejezetének áttanulmányozása alátámasztja a Précsényi Z. – Solymosi J. tanulmányában [79] leírtakat, miszerint *„Intézményi szinten mindössze két EU tagállamban sikerült olyan közigazgatási hatáskört azonosítani, amely a kritikus infrastruktúrák védelmének feladatkörére utal.”* [91]. Az Egyesült Királyság és a Német Szövetségi Köztársaság gyakorlatát érdemes górcső alá venni. Amit viszont semmilyen formában nem hagyhatunk figyelmen kívül az az Amerikai Egyesült Államok gyakorlata, hiszen egyrészt az információs társadalom kialakítása itt kezdődött meg a legkorábban azoknak az információs infrastruktúráknak a kiépítésével, amelyek e társadalom alapjait jelentik. Másrészt – pont az információs infrastruktúrák fejlettsége miatt – az infrastruktúrák védelmének kérdései is itt merültek fel először, mint nemzetbiztonsági kérdések.

[1] A NATO Parlamenti Közgyűlésének a biztonság polgári dimenziójával foglalkozó bizottság előadója, Lord Jopling a NATO 2007. tavaszi ülésére készített *„A kritikus infrastruktúrák védelme”* című jelentésében [78] is ezt a könyvet jelölte meg a kritikus információs infrastruktúrák védelméről szóló része forrásául. A jelentés áttekinti, melyek a létfontosságú infrastruktúrák, milyen fenyegetéssel kell szembenézniük, és a védelmükben milyen szerepet vállalhat a NATO és az Európai Unió. A jelentés célja a nemzeti parlamentek képviselőinek tájékoztatása az EU/NATO területén élő polgári lakosság védelmének legújabb fejleményeiről.

1.1. AZ ÉRTEKEZÉSBEN HASZNÁLT FOGALMAK

Napjainkban sem a kritikus infrastruktúra, sem a kritikus információs infrastruktúra fogalmának, és az ezzel szorosan összefüggő más fogalmaknak egységes, tudományos vagy szabványos, nemzetközileg, vagy akár hazai szinten elfogadott meghatározása nem létezik. Ennek megfelelően elsődleges szempont egy elfogadható meghatározás kidolgozása e fogalmakra, amely magának a védelmi körnek a definiálásából következhet. *„A kritikus infrastruktúrák veszélyeztetettségének feltérképezése, mérése, értékelése, s a szükséges védelmi intézkedések meghozatala előbb azt feltételezi, hogy a feltérképezéstől az intézkedésig egyetértés legyen abban, mi is az a kritikus infrastruktúra …”* [91]

1.1.1. AZ INFRASTRUKTÚRA ÉS A KRITIKUSSÁG FOGALMA

Első kérdésként az *infrastruktúra* fogalmát kell tisztázni. E fogalom esetében is számos – sok esetben egymást helyenként átfedő – meghatározással találkozhatunk.

A Magyar Értelmező Kéziszótár meghatározása szerint az infrastruktúra olyan angolszász eredetű szó, amely jelentése „*a társadalmi, gazdasági tevékenység zavartalanságát biztosító alapvető létesítmények, szervezetek (pl. lakások, közművek, a kereskedelem, a távközlés, az oktatás, az egészségügy stb.) rendszere.*” [79]

A Magyar Larousse Enciklopédia meghatározása szerint az infrastruktúra „*a társadalmi, gazdasági újratermelés zavartalanságát biztosító háttér. Legfontosabb elemei a közművek, az energiaellátás rendszere és a közlekedési, hírközlési hálózat (utak, vasutak, telefonhálózat, stb.) Az ún. lakossági infrastruktúrához tartozik a lakásállomány, a kereskedelmi és szolgáltatási hálózat, az egészségügyi, szociális, kulturális ellátás, az oktatás eszközei és intézményrendszere (kórházak, rendelőintézetek, iskolák).*” [80]

Egy másik meghatározás szerint az infrastruktúra nem más, mint „*egy adott rendszer (termelő vagy elosztó, szolgáltató rendszer, tudományos, állami, magán, nemzeti vagy nemzetközi szervezet, ország, város, vagy régió stb.) rendeltetésszerű működéséhez feltétlenül szükséges intézetek, intézmények, felszerelések és berendezések és a működtetést ellátó személyzet szabályszerűen működő összessége. Az infrastruktúra tehát a fizikai építményekből és berendezésekből és azokat szakszerűen működtetni tudó szakszemélyzetből áll.*” [48]

1997-ben egy, az akkori amerikai elnök, Bill Clinton utasítására létrehozott bizottság a következőképpen definiálta az infrastruktúra fogalmát (természetesen az Egyesült Államok vonatkozásában): „*Az infrastruktúrák olyan egymástól függő hálózatok és rendszerek*

összessége, amelyek meghatározott ipari létesítményeket, intézményeket (beleértve a szakembereket és eljárásokat), illetve elosztó képességeket tartalmaznak. Mindezek biztosítják a termékek megbízható áramlását az Egyesült Államok védelmi és gazdasági biztonságának fenntartása, valamint a minden szinten zavartalan kormányzati munka és a társadalom egésze érdekében." [32]

Megítélésem szerint ez utóbbi meghatározás fedi le legjobban mindazokat a tényezőket, amelyekkel kutatásaim során, mint az infrastruktúra fogalomkörébe tartozónak tekintettem. Ennek megfelelően **értekezésemben e definíciót** fogadtam el és használtam az **infrastruktúra vonatkozásában.**

A magyar nyelv szabályait és szokásait a legmesszebb menőkig figyelembe kell venni (és ettől eddigi publikációimban ritkán tértem el), de akadnak olyan esetek is, amikor ez nem tűnik célszerűnek. A kritikus információs infrastruktúra kifejezés is meglehetősen pontatlannak tűnik. Már a *kritikus* jelző használata sem a legjobb, hiszen nem az infrastruktúra a kritikus, **hanem annak elvesztése, sérülése válhat kritikussá,** ezért célszerűbb lenne a – néhány fordításban használt – *létfontosságú* kifejezést használni. Az információs infrastruktúra sem igazán szabatos kifejezés magyarul, mert abba például a könyvtárakat is bele kell érteni, holott mindenki érti és érzi, hogy itt nem információs, hanem elektronikus információs infrastruktúrákról van szó. Ennek ellenére e doktori értekezés keretein belül, az egységes szóhasználat és értelmezés kedvéért a *kritikus információs infrastruktúra* kifejezést használom, mivel az elmúlt években így honosodott meg, holott az – az előzőekben megfogalmazottak szerint – valójában *létfontosságú elektronikus információs infrastruktúrá*t jelent.

1.1.2. A VÉDELEM ÉS A BIZTONSÁG FOGALMÁNAK MEGHATÁROZÁSA

Ahhoz, hogy a kritikus infrastruktúrák és kritikus információs infrastruktúrák védelméről tárgyaljunk, tisztáznunk kell a védelemnek és a biztonságnak – mint legszélesebb osztálynak – a fogalmát és tartalmát. A legszélesebb osztály a mi esetünkben a védelem és a biztonság fogalma. A védelem – a magyar nyelvben – tevékenység, illetve tevékenységek sorozata, amely arra irányul, hogy megteremtse, fejlessze, vagy szinten tartsa azt az állapot, amit biztonságnak nevezünk. Tehát a védelem tevékenység, amíg a biztonság egy állapot. Az

(amerikai) angol nem tesz különbséget a biztonság és a védelem között, általában mindkettőre a security[2] szót használja[3].

A biztonság értelmét, tartalmát sokan sokféleképpen magyarázzák. Azt hiszem, hogy *„A biztonság olyan kedvező állapot, amelynek megváltozása nem valószínű, de nem is zárható ki ..."* [34] megfogalmazás értelmetlensége magyarázatot nem igényel. A Magyar Értelmező Kéziszótár szerint *„a biztonság veszélytől, vagy bántódástól mentes, zavartalan állapot"* [79]. Ezt a megfogalmazást is elég nehéz tudományos és műszaki szemlélettel elfogadni, mert zavartalan állapot – mint tudjuk – nem létezik, másrészt nem a zavar teljes hiánya, hanem valamilyen *még elviselhető* mértéke és bekövetkezésének gyakorisága az, ami már valamilyen szinten biztonságnak tekinthető.

Elfogadva, hogy a biztonság egy *kedvező állapot*, amellyel szemben elvárható, hogy a fenyegetések bekövetkezésének lehetősége, valamint az esetlegesen bekövetkező fenyegetés által okozott kár a lehető legkisebb legyen. Ahhoz azonban, hogy teljes legyen ez a biztonság az szükséges, hogy minden valós fenyegetésre valamilyen védelmet nyújtson, ugyanakkor körkörös legyen, vagyis minden támadható ponton biztosítson valamilyen akadályt a támadó számára. Mindezek mellett elvárható, hogy folyamatosan létezzen. [85]

A biztonság, mint állapot magyar nyelvű értelmezését több mint tíz éve az *Informatikai Rendszerek Biztonsági Követelményei* című MeH ITB[4] 12. számú ajánlás [82] készítése során alkottuk meg Bodlaki Ákos kollégámmal, majd ezt *Az informatikai biztonság kézikönyve* című műben [85] tovább finomítottam. A fentiek alapján a kritikus infrastruktúrák és kritikus információs infrastruktúrák, az informatika és a kommunikáció területén folytatott kutatásaim során a védelmet és biztonságot a következőképpen értelmezem:

A védelem a biztonság megteremtésére, szinten tartására, fejlesztésére irányuló tevékenység.

---

[2] A biztonságra a safety szót is használja környezet-, munka- és egészségvédelmi dimenzióban.

[3] A protection ugyan védelmet jelent, de azt ritkán (például data protection – a személyes adatok védelme) használja a szakirodalom.

[4] Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság

A biztonság a rendszer olyan – az érintett[5] számára kielégítő mértékű – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Ahol a **zárt védelem** az összes releváns fenyegetést figyelembe vevő védelmet, a **teljes körű védelem** pedig a rendszer valamennyi elemére kiterjedő védelmi intézkedések összességét jelenti. A **folytonos védelem** az időben változó körülmények és viszonyok ellenére is megszakítás nélkül valósul meg. A **kockázattal arányos védelem** esetén egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel, azaz a védelemre akkora összeget és olymódon fordítanak, hogy ezzel a kockázat az érintett számára még elviselhető, vagy annál kisebb.

A *kockázat* szó a köznyelvben nagyon elterjedt, de fogalmának leírására, a felhasználási területtől és a kiválasztott módszertől függően, feldolgozhatatlan mennyiségű leírása létezik. A kockázat, a kockázatelemzés kérdéseire itt nincs lehetőség kitérni, de a problémának a szakterületre vonatkozó elemzését tartalmazzák többek között a [26] és [25] munkák, ahol a kritikus infrastruktúrák védelmének megközelítésében (is) tárgyalják a szerzők a biztonsági szakterületen a kockázatelemzés kérdéseit, problémáját. Bukovics I. –Vavrik A. többek között megállapítja, hogy *„A nemkívánt esemény – egy blackout – egy kritikus esemény mindig egyedi, egyszeri, azonos körülmények között meg nem ismételhető, nem stochasztikus, bár lehet tömegjelenség (de nem véletlen tömegjelenség) is. Ezért tehát kívül esik a valószínűségszámítás érvényességi körén. A valószínűségi kockázatelemzés körén is. … "Egy egyszeri véletlen eseménnyel kapcsolatban a tudomány nem tehet többet, mint hogy megállapítja annak véletlen jellegét." [93] … A tudomány nem tagadhatja, és nem ignorálhatja, hogy az egyszeri eseménynek is lehet kockázata …”* [25].

Ezen megállapítások a kockázatelemzés kérdéseinek megközelítését nem könnyítik meg, de ugyanakkor rávilágítanak arra, hogy érdemes mindig a feladat céljának megfelelő definíciót választani. A kockázatot sokan sokféleképpen definiálják, a különböző sztochasztikus és determinisztikus kockázati modellek nagyon komoly matematikai alapokon nyugszanak, azonban többszörösen összetett rendszerek esetében ezek a modellek a gyakorlatban nehezen használhatók.

[5] Az *érintett* alatt a védelem nem kielégítő megvalósítását elszenvedő, a védelmet előíró, továbbá a védelemért felelős személyek és szervezetek együttese értendő. (Eredetileg a [82]-ben, majd a [85]-ban a játékelméleti definícióból származó *védő* kifejezés szerepelt.)

Még 1995-ben a MeH ITB megrendelésére, a CRAMM[6] módszertanon alapuló MeH ITB 8. számú ajánlása [83] segítségével végzett kockázatelemzések során – a CRAMM módszertannal összhangban – Marx György akadémikus következő definíciójából [81] indultunk ki. *„A kockázat* (rizikó, riszk – mint reszkíroz) *matematikai értelmezése a következő*:

$$R = W \times K, \qquad (1)$$

ahol W *a bekövetkezés valószínűsége,* K *pedig a következmény súlyossága."* Ebből származik az *Informatikai Rendszerek Biztonsági Követelményei* című MeH ITB ajánlásban [82] leírt meghatározás

$$r = \sum_{t \in T} \left(p_t \times d_t \right), \qquad (2)$$

ahol: **r**: a rendszer biztonsági kockázata [pl.: Ft/év],

T: a releváns fenyegetések halmaza,

$\mathbf{p_t}$: egy adott fenyegetés bekövetkezésének valószínűsége [pl.: 1/év],

$\mathbf{d_t}$: egy adott fenyegetés bekövetkezéséből származó kár [pl.: Ft].

A fenti meghatározást nem csak egyszerűsége és átláthatósága végett fogadtuk el, hanem azért is, mert a biztonság definiálása során elfogadott kiindulóponttal[7] is összhangban van, továbbá – a sztochasztikus vagy a determinisztikus kockázati modellekhez viszonyított – pontatlansága ellenére a kvalitatív kockázatelemzéseknél[8] a gyakorlatban felhasználható.

1.1.3. AZ INFOKOMMUNIKÁCIÓ ÉS AZ INFOKOMMUNIKÁCIÓS BIZTONSÁG

Az informatikai, a kommunikációs, és az egyéb elektronikus rendszerek között az egyes rendszerek kommunikációs vagy informatikai rendszerként való meghatározása egyre

[6] A brit kormány Központi Számítógép és Távközlési Ügynökség (Central Computer and Telecommunications Agency) *CCTA Risk Analysis and Management Method* kockázatelemzési és kezelési módszertana. [51]

[7] A biztonság egy kedvező állapot, amellyel szemben elvárható, hogy a fenyegetések bekövetkezésének lehetősége, valamint az esetlegesen bekövetkező fenyegetés által okozott kár a lehető legkisebb legyen.

[8] Összetett rendszerek biztonsági kockázatainak vizsgálatához általában a kvalitatív kockázatelemzés kielégítő eredményt ad. Amennyiben kvantitatív kockázatelemzést kell végezni, a kockázat fenti definíciója – pontatlansága miatt – nem alkalmazható.

nehezebb[9]. E technológiák konvergenciáját az informatikával és a távközléssel foglalkozó szakemberek már több mint egy évtizede vizsgálják. Az információs társadalomhoz és a médiához kötődő iparágak konvergenciáját már az Európai Unió 1997-ben kiadott, *Zöld Könyv a távközlési, média és informatikai ágazatok konvergenciájáról és annak szabályozási kihatásairól* [44] leírta, később pedig – az újabb fejleményeket is figyelembe véve – az európai audiovizuális politika szabályozásának jövőjéről szóló 2003-as közlemény aktualizálta. A közlemény megállapítja, hogy *„Az információs társadalom fordulóponthoz érkezett: az elmúlt időszakban hatalmas technológiai fejlődés zajlott le, és az IKT[10] napjainkban lép a tömeges alkalmazás szakaszába ... Műszaki szempontból a távközlési hálózatok, a médiumok, a tartalom, a szolgáltatások és az eszközök digitális konvergenciájával állunk szemben. ... Az* ***információs társadalom és a média területén működő szolgáltatások, hálózatok és eszközök digitális konvergenciája*** *végre mindennapjaink valóságává válik ... A technológiában zajló alapvető változások ... a* ***politikában*** *is* ***konvergenciát*** *tesz szükségessé, és késznek kell lenni arra, hogy a szabályozási keretet a kialakulófélben lévő digitális gazdaság igényei szerint alakítsuk”*. [17]

Sokszor csak a számítógép- és távközlési rendszereket értik ez alatt, de ténylegesen ide tartozónak kell tekintenünk minden olyan elektronikus eszközt vagy rendszert, amely adatok[11] feldolgozására szolgál.

Az informatikai és kommunikációs technológiák[12] fent bemutatott konvergenciája miatt általában az *informatikai és kommunikációs technológia*, az *informatikai és kommunikációs rendszerek* kifejezéseket használják, de újabban egyre gyakrabban alkalmazzák az infokommunikációs technológia, vagy az infokommunikációs rendszerek kifejezést is. A továbbiakban e kifejezést fogom az értekezésben használni, és annak meghatározását a következőképpen fogadom el:

---

[9] A telefonközpontok egy speciális számítógépként, a routerek telefonközpontként is felfoghatók. Egy mobiltelefonként is használható, Wi-Fi, GPRS és Bluetoth kapcsolatokkal rendelkező, GPS-el felszerelt zsebszámítógép, egy PDA szakszerű besorolása, pedig igencsak nehéz feladat. (lásd még [45])

[10] IKT: információs és kommunikációs technológiák

[11] Adat: Az információnak olyan új formában való ábrázolása, amely alkalmas közlésre, értelmezésre, vagy feldolgozásra. Tények, fogalmak vagy utasítások formalizált ábrázolása, amely alkalmas az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra. Információ: Bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságot csökkent vagy szüntet meg.[84]

[12] angolul: Information and Communications Technology (ICT), néha az Information and Related Technology kifejezést is használják.

Infokommunikációs rendszer alatt az adatok gyűjtésére, felvételére, tárolására, feldolgozására (megváltoztatására, átalakítására, összegzésére, elemzésére, stb.), továbbítására, törlésére, hasznosítására (ideértve például a nyilvánosságra hozatalt is)**, és felhasználásuk megakadályozására használt elektronikus eszközök, eljárások, valamint az üzemeltető és a felhasználó személyek együttesét értem.**

Ezek alapján az infokommunikációs rendszerekhez tartoznak:

1. az informatikai rendszerek és hálózatok, ide értve az internet szolgáltatást is;
2. a vezetékes, a mobil, a rádiós és műholdas távközlés;
3. a vezetékes, a rádiófrekvenciás és műholdas műsorszórás;
4. a rádiós vagy műholdas navigáció;
5. az automatizálási, vezérlési és ellenőrzési rendszerek (SCADA[13], távmérő, távérzékelő és telemetriai rendszerek, stb.);
6. a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.

Amint a későbbiekben részletesen is bemutatom, a kritikus infrastruktúra elemek szerves részét képezik az egyes elemek infokommunikációs rendszerei, illetve a kritikus információs infrastruktúrák különböző, egymáshoz kapcsolódó infokommunikációs rendszerekből állnak. Ezért az egyes kritikus infrastruktúra elemek szempontjából az infokommunikációs rendszerek védelmét (is) meg kell valósítani. Így elengedhetetlen, hogy ennek biztonságát is értelmezzük.

Az infokommunikációs rendszerek biztonsága szükségességének felismerése már jóval a kritikus információs infrastruktúrák védelmi igényének megjelenése előtt megtörtént, de sokáig elkülönülve kezelték és értelmezték. A kommunikáció biztonságának egyik nagyon régi ága a kriptográfia, a rejtjelzés tudománya, de az informatikai rendszerek biztonsága szükségességének felismerése sem új keletű[14]. Ezek a védelmi igények például a NATO szabályrendszerei között is megjelentek.

---

[13] Supervisory Control and Data Acquisition (System) – felügyelet-irányítás és adatgyűjtés (rendszerek)

[14] Az Amerikai Egyesült Államokban már a hetvenes években a légierő már olyan mértékben használta a számítógépeket, hogy azok biztonsága, a „computer security” iránti igény megjelent, és tudományos munkákat dolgoztattak ki e téren. Ennek talán egyik legemlékezetesebb alkotása Bell és LaPadula műve [35]. A Bell-LaPadula tétel a mai napig is a formálisan bizonyított és ellenőrzött hozzáférés-védelem alaptétele. Az informatikai biztonság iránti „nyilvános igényt” az Amerikai Egyesült Államok Védelmi Minisztériuma által (először) 1983-ben kiadott TCSEC (Trusted Computer System Evaluation Criteria, amely a szakirodalomban még az Orange Book, a Narancs könyv néven is ismert) [36] jelentette, amelyet sorra követtek a különböző ajánlások és szabványok.

A NATO védelmi előírása szerint *„Az információvédelem az általános védelmi rendszabályok és eljárások alkalmazása, az információ megsemmisülésének vagy kompromittálódásának megelőzése, felfedése ellen és helyreállítása céljából.”*. [95] Ettől megkülönbözteti az úgynevezett INFOSEC[15]-et, amely *„a biztonsági rendszabályok alkalmazása a kommunikációs, információs és más elektronikus rendszerekben a feldolgozott, tárolt vagy továbbított információ bizalmasságának, sértetlenségének vagy rendelkezésre állásának véletlen vagy szándékos elvesztése ellen, és e rendszerek sértetlenségének vagy rendelkezésre állásának elvesztése ellen.”* [95] Ez gyakorlatilag megegyezik Európai Unió Tanácsának Biztonsági Szabályzata [41] előírásaival. Jól érzékelhető, hogy az információvédelem általában, mindenféle információ védelméről szól. Az INFOSEC része az információvédelemnek, és egyértelműen a kommunikációs, információs és más elektronikus rendszerekre vonatkozik.

A civil szférában egyre inkább terjedő, és elfogadottá váló *ISO/IEC 27001:2005 szabvány* szerint: *„Az informatikai biztonságot[16] az jellemezi, hogy megőrzi ... a bizalmasságot ...; a sértetlenséget ...; a rendelkezésre állást ...”*[17]. [65] Egy szabványhoz képest kissé pongyola a meghatározás, mert nem derül ki, hogy minek a bizalmasságát, sértetlenségét vagy rendelkezésre állását kell megőrizni.

Az információbiztonságot és az informatikai biztonságot – néha még a szakemberek is – gyakran összekeverik egymással, sőt időnként az adatvédelemmel is. [37] Az adatvédelem kifejezés – érdekes módon az angol nyelvben (data protection) is – a személyes adatok védelmére vonatkozik, a személyiségi jogokkal összefüggő tevékenység. Az információbiztonság és az informatikai biztonság különbözik egymástól. Az információbiztonság a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt adatok védelmére vonatkozik.

---

[15] INFOSEC: information security (ang.), az általánosabb értelmű információbiztonságtól való megkülönböztetés érdekében használt kifejezés. Magyar fordítása: elektronikus dokumentumvédelem.

[16] A szabvány címének első része angolul: Information Technology, franciául: Technologies de d'information, németül: Informationstechnologie, ezért az Information Technology kifejezést informatikaként fordítottam.

[17] angolul: *Information security is characterized here as the preservation of: a) confidentiality ...; b) integrity ...; c) availability…*

Ezzel szemben például az informatikai biztonság[18] csak az informatikai rendszerekben kezelt adatok, és az azt kezelő rendszer védelmét jelenti. Mivel angolul általában az információvédelemre, illetve az informatikai védelemre, sőt néha a kommunikációs, információs és más elektronikus rendszerek védelmére is az *information security* kifejezést használják, az egyes fordítások még inkább zavarossá teszik a képet. Általában a szövegkörnyezet egyértelművé teszi, hogy információvédelemről vagy informatikai védelemről van szó, de a NATO az egyértelműség kedvéért bevezette az INFOSEC kifejezést, amelyet az *information security* kifejezés szavainak összevonásával (INFOrmation SECurity) képeztek. Ezt a vonatkozó magyar irodalmakban általában *elektronikus információvédelem* formában használnak.

A kérdés problematikus voltát a témához kapcsolódó doktori értekezés-tervezetében Kassai Károly a következőképpen mutatja be: *„Információbiztonság területén a dokumentumok, jogszabályok, publikációk és egyéb források (pl. szabványok, ajánlások, kézikönyvek) eltérő szakkifejezéseket alkalmaznak, mutatva, hogy hazánkban még nem alakult ki egységes nyelvezet. A magyar katonai terminológia információbiztonság területén kidolgozatlannak ... tekinthető, aminek következménye a doktrínákban tapasztalható fogalmi pontatlanság."* [76]

Az információvédelemre a NATO védelmi előírása [95] némi kiegészítéssel tökéletesen elfogadható. *Az információvédelem az általános védelmi rendszabályok és eljárások alkalmazása* ***a bármilyen formában, szóban, rajzban, írásban, az infokommunikációs rendszerekben kezelt***[19] *információ megsemmisülésének vagy kompromittálódásának megelőzése, felfedése ellen és helyreállítása céljából.* Gyakorlati tapasztalataim szerint az információvédelem területeit a NATO által meghatározattak majdnem tökéletesen fedik le.

[18] Az informatikai biztonság fogalmát a *MeH ITB 12. sz. ajánlás* [82] készítése során meghatároztuk. Akkor még a nemzetközi szakirodalmat figyelembe véve az informatikai rendszerben kezelt adatok bizalmasságát, sértetlenségét, hitelességét, funkcionalitását és rendelkezésre állását, valamint az informatikai rendszer elemeinek funkcionalitását és rendelkezésre állását tekintettük védendőnek. Később ezt a [85] műben tovább fejlesztve – a nemzetközi szakirodalmat figyelembe véve – csak a bizalmasságot, sértetlenséget és rendelkezésre állást tekintettem védendő értéknek.

[19] Adatok kezelése: gyűjtés, felvétel, tárolás, feldolgozás (megváltoztatás, átalakítás, összegzés, elemzés, stb.), továbbítás, törlés, hasznosítás (ideértve például a nyilvánosságra hozatalt is), és felhasználásuk megakadályozása.

Ezek a területek: [98]

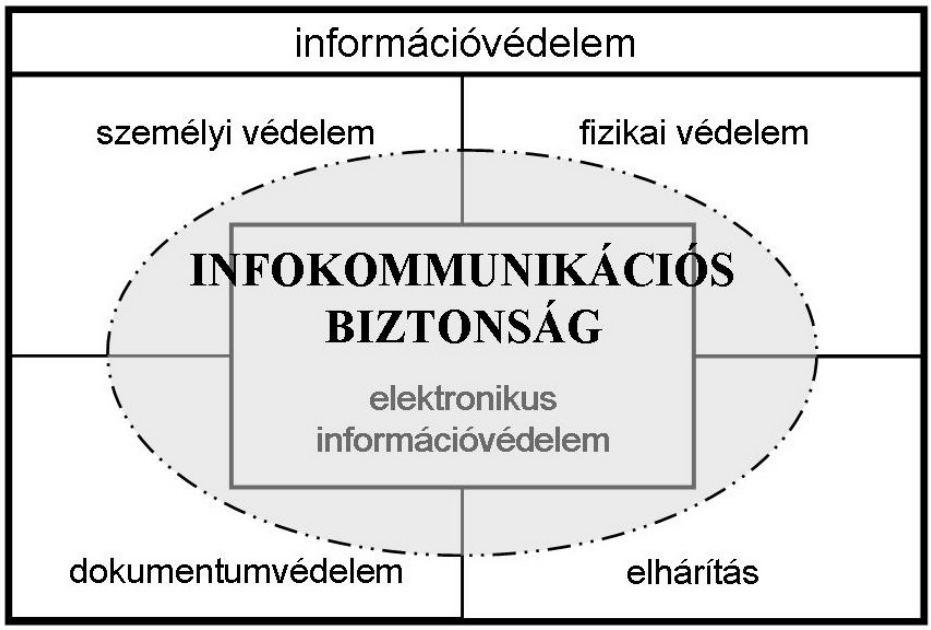
- a személyi védelem;
- a dokumentumvédelem;
- a fizikai védelem;
- az elhárítás (felderítés elleni tevékenység) és
- az elektronikus információvédelem.

Az elektronikus információvédelem esetében nem egyértelmű, hogy az minden infokommunikációs rendszerre (és az abban kezelt adatokra) vonatkozik-e? Nem egyértelmű, hogy a rádiós vagy műholdas navigáció, az automatizálási, vezérlési és ellenőrzési rendszerek, a felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek nem informatikai vagy kommunikációs alrendszerein túl is ide tartoznak vagy sem? A vezetékes, a rádiófrekvenciás és műholdas műsorszórás, pedig biztos, hogy nem érthető bele az elektronikus információvédelembe.

A polgári szférában a mindenre kiterjedő információvédelmet többnyire nem tudják, és nem akarják megvalósítani, de az infokommunikációs rendszerekben kezelt adatok védelme számukra is fontos. Ezért jelent meg korábban az informatikai biztonság kérdése, és ezért érdemes a fentieket összevetve meghatározni – az infokommunikáció értelmezése mellett annak biztonságát – az infokommunikációs biztonság fogalmát. Ez – megítélésem szerint – a kritikus információs infrastruktúrák védelmével kapcsolatosan jól hasznosítható.

Az infokommunikációs védelem az információvédelemnél szűkebb, az infokommunikációs rendszerekre és az azokban kezelt adatok védelmére vonatkozik. A biztonság eléréséhez a védelemnek ez esetben is ki kell terjedni az infokommunikációs rendszer valamennyi elemére[20], de nem a teljes információs rendszerre. A személyi védelem, a dokumentumvédelem, a fizikai védelem és az elhárítás (felderítés elleni tevékenység) az infokommunikációs rendszer elemei vonatkozásában értelmezésre kell, hogy kerüljön, de nem alkalmazzuk önállóan, és csak az infokommunikációs rendszer védelme vonatkozásában, annak fenyegetései ellen. Az infokommunikációs biztonság és a NATO értelmezése szerinti [95] információvédelem egymáshoz való viszonyát az 1. ábra mutatja be.

[20] Rendszerelemek: az infokommunikációs rendszer környezetét alkotó és működéséhez szükséges infrastruktúra (pl.[101]), az infokommunikációs rendszer hardver, szoftver és kommunikációs elemei, az adathordozók, az input és output dokumentumok, a rendszerre vonatkozó dokumentációk, és az infokommunikációs rendszer kezelői, kiszolgálói és felhasználói. [82]



1. ábra – Az infokommunikációs biztonság és az információvédelem [szerk.: Muha Lajos]

A biztonság korábbi meghatározását elfogadva, ennek általános értelmezéséből levezethetjük az infokommunikációs biztonság fogalmát. Ehhez kiindulópont, hogy **a védelem egyik tárgya az *adat,*** amely az információnak közlésre, értelmezésre, vagy feldolgozásra alkalmas ábrázolása. [84] A fenyegetések az *adatok bizalmasságát, sértetlenségét és rendelkezésre állását* veszélyeztetik, de nem közvetlenül érik az adatokat, hanem az azokat kezelő *rendszerelemeken* (pl. a hardver, szoftver, hálózat, személyek, …) keresztül érvényesülnek. Ennek figyelembe vételével, a biztonság általános definíciója alapján az infokommunikációs biztonságot a következőképpen határozom meg:

Az infokommunikációs biztonság az infokommunikációs rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelynek védelme az infokommunikációs rendszerben kezelt[21] adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

A fenti meghatározás több szempontból megegyezik, több szempontból különbözik a NATO INFOSEC meghatározásától. Megegyezik a két meghatározás abban, hogy mindkettő

[21] Az adatok kezelése az alkalmazott eljárástól függetlenül a adatok gyűjtése, felvétele, tárolása, feldolgozása (megváltoztatás, átalakítás, összegzés, elemzés, stb.), továbbítása, törlése, hasznosítása (ideértve például a nyilvánosságra hozatalt is), és felhasználásuk megakadályozása.

kommunikációs, informatikai és más elektronikus rendszerekre és az azokban kezelt adatokra vonatkozik. Az eltérés az alábbiakban összegezhető:

1. a biztonsági rendszabályok a kommunikációs, informatikai és más elektronikus rendszerekben a feldolgozott, tárolt vagy továbbított adatok bizalmasságának, sértetlenségének vagy rendelkezésre állásának véletlen vagy szándékos elvesztése megakadályozására, és e rendszerek sértetlenségének vagy rendelkezésre állásának biztosítására irányulnak;
2. a biztonságot, mint állapotot határoztam meg, amely magába foglal védelmi eljárásokat (zárt, teljes körű, folytonos és a kockázatokkal arányos) is;
3. a védelem egyértelműen kiterjed az infokommunikációs rendszer valamennyi elemére is.

1.2. A KRITIKUS INFRASTRUKTÚRÁK MEGHATÁROZÁSI MÓDSZEREI

A kritikus infrastruktúrák meghatározásához három tényező alkalmazását javasolja számos ezzel a kérdéssel foglalkozó irodalom [23], [32], [100]:

– **Hatókör**: földrajzi kiterjedésben mutatja a kritikus infrastruktúra (vagy részének) megsemmisülése, működésképtelenné válásának hatását. Ez lehet nemzetközi, nemzeti, regionális, territoriális vagy helyi.
– **Nagyságrend**: a veszteség vagy a hatás nagyságrendje (például: nincs hatás, minimális, mérsékelt vagy jelentős a hatás). A nagyságrend megállapításához a következő szempontokat is érdemes figyelembe venni:
  - népességre gyakorolt hatás (az érintett lakosság száma, áldozatok, betegségek, súlyos sérülések, kitelepítések);
  - gazdasági hatás (GDP-re gyakorolt hatása, jelentős gazdasági veszteség és/vagy termelés, szolgáltatás fokozatos romlása);
  - környezetvédelmi (a lakosságra és lakókörnyezetére gyakorolt hatás);
  - interdependencia (a kritikus infrastruktúrák elemei közötti függőség);
  - politikai (az államba vetett bizalom).
– **Időbeli hatás**: mely megmutatja, hogy az adott infrastruktúra vagy elemének vesztesége mennyi idővel később fejti ki komoly hatását (pl.: azonnali, 24-48 óra, egy hét, egyéb).

A kritikus infrastruktúrák meghatározása után be kell azonosítani az infrastruktúrák azon elemeit, amelyek létfontosságúak az adott infrastruktúra működéséhez, illetve amelyek a

legjelentősebb életveszélyt vagy gazdasági veszélyt okozhatják. **A kritikus infrastruktúráknak ugyanis nem minden eleme tekinthető kritikusnak.** Az infrastruktúrák mérete és összetettsége segíthet beazonosítani a kritikus elemeket.

Természetesen egyfajta **priorálást** is végre kell hajtani az infrastruktúrák között. A priorálás alábbi módozatainak a következőket választottam:

1. A **ténylegesen kritikus létesítmények** és eszközök beazonosítása, és
   - felkészíteni a támadás lehetőségére, vagy megnehezíteni a hozzáférést;
   - veszteség hatását csökkenteni további elemek beépítésével vagy újratervezéssel, vagy áthelyezéssel.
2. Beazonosítani olyan **sérülékenységeket és/vagy megoldásokat melyek több mint egy infrastruktúrát érintenek**. (ilyenek például az infokommunikációs rendszerek). Az infokommunikációs rendszerek sérülékenységeinek megoldásai általánosságban alkalmazhatók:
   - a legjobb gyakorlat (best practice) alkalmazásával;
   - biztonságosabb szoftverek kifejlesztésével.

   Ugyanígy több infrastruktúrát érintő technológia az irányítási kontroll rendszerek (pl. SCADA).
3. **Infrastruktúrák közötti interdependenciák beazonosítása**. Az eddig említett infrastruktúrák egyike sem teljesen izolált más rendszerektől. Emiatt az infrastruktúra egy elemének támadása esetén veszélyes hatás alakulhat ki más infrastruktúrában.
4. **Földrajzi elhelyezkedés** szerint, azok a területek, ahol egynél több infrastruktúra helyezkedik el, elsőséget igényelhet.
5. **Tulajdonviszonyok alapján:** az állam által tulajdonolt és működtetett infrastruktúrák, vagy magánkézben lévő infrastruktúrák, melyek az állami szolgáltatások nyújtásához szükségesek, vagy amellyel az államnak tradicionális együttműködése van, elsőbbségeket élvezhetnek.

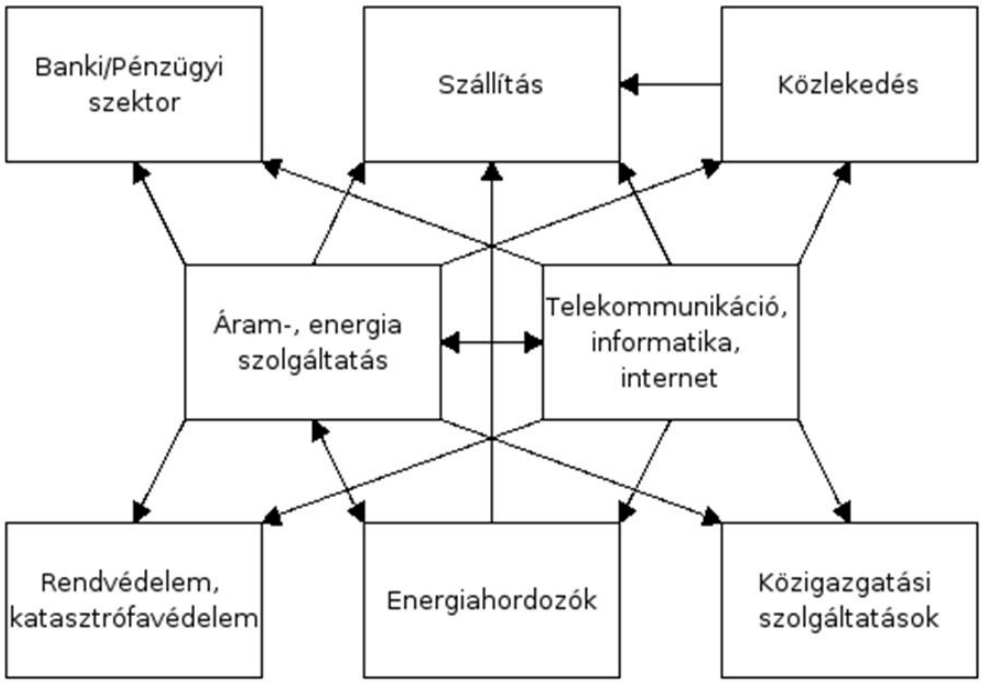
Véleményem szerint, amikor a későbbiekben meg kívánom határozni hazánk kritikus információs infrastruktúráit, akkor a fenti besorolási tényezőket kell figyelembe venni.

Ennek során a hatókör szempontjából a Magyar Köztársaság kritikus információs infrastruktúráit az országra gyakorolt hatásuk alapján kell kijelölni.

A nagyságrend figyelembe vétele során a jelentős hatású veszteségék a mérvadóak, de a közepes vagy mérsékelt hatás esetén vizsgálni kell annak időbeli hatását is. Amennyiben a hatás hosszabb távon fennmarad, például maradandó környezetkárosodás, a hatásában alacsonyabb nagyságrendű infrastruktúrák is a közepesek közé sorolandók.

1.2.1. A KRITIKUS INFRASTRUKTÚRÁK INTER- ÉS INTRADEPENDENCIÁJA

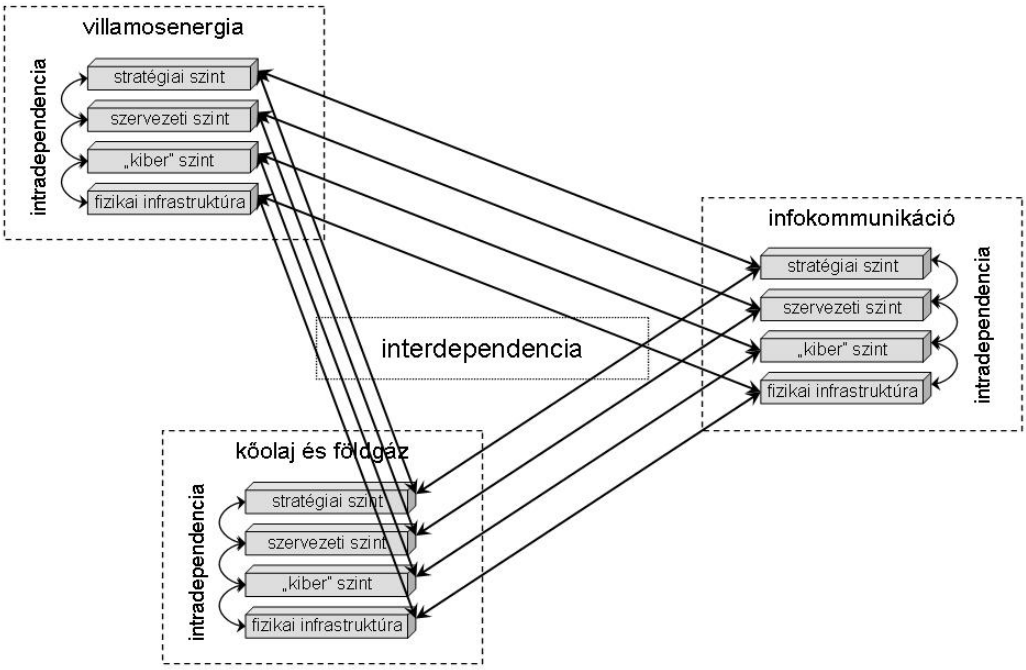
Mint a fentiekben már említésre került, az infrastruktúrák nem elszigetelten működnek, hanem egymással – gyakran nagyon szoros – kölcsönhatásban állnak (2. ábra). Ezt a jelenséget nevezi a szakirodalom interdependenciának.



2. ábra – A kritikus infrastruktúra elemeinek interdependenciája [23]

Az összekapcsolódó infrastruktúrákon keresztül a problémák felhalmozódhatnak, váratlanabb és lényegesen súlyosabb működésbeli zavart okozhatnak az adott állam létfontosságú szolgáltatásaiban. Az infrastruktúrák összekapcsolódásai, és egymástól való függőségei sérülékenyebbé teszi őket támadások, zavarok, megsemmisítésre irányuló tevékenységekkel szemben. Például az energiatermelés függ a szállítástól. A szállítás függ az energiától. Mindkettő függ az infokommunikációs rendszerektől, míg az infokommunikációs rendszerek energiafüggők (2. ábra). A rendszerben az energia- és áramszolgáltatást, valamint az infokommunikációs infrastruktúrát kritikus infrastruktúrának tekintjük. A létfontosságú szolgáltatások infrastruktúráktól függnek, illetve némely infrastruktúra függhet más szolgáltatásoktól is.[56]

Az infrastruktúra elemei, melyet eszközökként jelenítettünk meg, sérülékenyek. Az infrastruktúra fenyegetettségei a sérülékenységeket használják ki. A sérülékenységek mentén jelentkező fenyegetettség elhárítása vagy csökkentése meghatározott stratégiákkal valósítható meg.



3. ábra – Az inter- és az intradependencia összefüggése [22]

A kritikus infrastruktúrák információs rendszerei esetében az intradependencia hatása is rendkívül jelentős. Egy-egy adott infrastruktúra stabilitása jelentős mértékben függ az információs rendszerének biztonságától, amit a hagyományos infokommunikációs biztonsági eszközökkel, különösen az informatikai biztonsági irányítási rendszer[22] bevezetésével és működtetésével tudunk befolyásolni. [22]

Megítélésem szerint az infrastruktúrák belső és külső függőségeinek vizsgálata mind az infrastruktúrák besorolása, mind a védelmi intézkedések kialakítása során nagy jelentőséget kell, hogy kapjon. Az előzőekben leírtak következtében egy adott ország – így Magyarország esetében is – kritikus infrastruktúrájának meghatározásakor a vizsgálatnak ki kell terjednie az infrastruktúrák interdependenciájára és intradependenciájára egyaránt.

1.2.2. AZ INFRASTRUKTÚRÁK TULAJDONI VISZONYAI

A kritikus fontosságú infrastruktúrák tulajdonosi megoszlása eltérő lehet. Központi, minisztériumok vagy szervezeteik által használt rendszerek, a honvédelmi és rendvédelmi szervek tulajdonában lévő számítógépes és távközlési hálózatok, az egészségügyben adminisztrációra és elszámolásra kiépült számítógépes rendszerek, állami tulajdonú vállalatok

[22] Informatikai Biztonsági Irányítási Rendszerek – Information Security Managament Systems (ISMS). [65]

(pl. repülőtérek) kritikus rendszerei általában állami, önkormányzati tulajdonban vannak. Azonban több kritikus infrastruktúra is tartozhat a magánszektorhoz, melyek között az alapot jelentő távközlési és helyi áramszolgáltatók is megtalálhatóak.

Természetesen a helyzet ennél még összetettebb lehet. Számos lehetőség áll rendelkezésre az infrastruktúra tulajdonos szervezet részére, hogy infrastruktúráját más cég által üzemeltesse, vagy teljesen kiszervezze[23], de az is előfordulhat, hogy az infrastruktúrát szolgáltató saját infokommunikációs hálózattal rendelkezik ugyan, de az eszközök beszállítóitól nagymértékben függ.

Az infrastrukturális üzleti világ annyiban különbözik a többi üzleti világtól, hogy ez esetben a folyamatos ellátottsághoz fűződő fogyasztói érdek erősebb lehet, mint az ahhoz fűződő kereskedelmi érdek. Ez különösen problémás lehet ott, ahol az infrastruktúra szolgáltatója monopolhelyzetben van, hiszen nincs, vagy csökkent mértékű a versenyhelyzetből eredő nyomás a rendszer fenntartására. Erre jó példa lehet egy olyan áramszolgáltató társaság, amely idő és megfelelő pénzalapok nélkül inkább kockáztatja a szolgáltatásban bekövetkezhető leállásokat, és inkább olyan területeken fejleszt, mely nyereséget hozhat neki, ahelyett, hogy a folyamatos ellátás érdekében fejlesztené infrastruktúráját.

Tekintettel a magánszektor infrastruktúra biztonságával szemben fennálló, a fentebb kifejtett félelmekre, a kormányzatnak figyelembe kell vennie, hogy hogyan biztosíthatja a hatékony kockázatmenedzsmentet ilyen esetekben. Logikus megközelítése a kérdésnek a felelősségi határok megállapítása. Azaz szabályozni kell, hogy meddig kezelik a kockázatokat az infrastruktúra tulajdonosai, és mikor következik e kérdésben az állami szerepvállalás.

Véleményem szerint, a tulajdonviszonyok figyelembe vétele, úgy az egyes infrastruktúrák kijelölése során, mint azok más infrastruktúrákra gyakorolt hatásának vizsgálata szempontjából rendkívül fontos hazánkban, mert a tulajdoni viszonyokra a magántulajdon a jellemző, és ez a védelem megvalósítása során más kezelést igényel, mint az állami tulajdon. Ez a kérdéskör viszont felveti a **pontos törvényi előírások szükségességét,** valamint ezen túl a kölcsönös érdekek keresését, mert a magánszféra érdekeltségének megteremtésével már nem csak számon kérhetővé válnak a védelmi intézkedések, hanem valós együttműködés is kialakítható.

[23] tevékenységek kiszervezése, más szóval vállalkozásba adása, ang.: outsourcing

1.3. KRITIKUS INFRASTRUKTÚRA MEGHATÁROZÁSOK KÜLÖNBÖZŐ ORSZÁGOKBAN ÉS SZERVEZETEKBEN

1.3.1. AZ EURÓPAI UNIÓ KRITIKUS INFRASTRUKTÚRA MEGHATÁROZÁSA

Kritikus infrastruktúrának az Európai Unióban (EU) több meghatározása létezik. Ez jelentős részben – mint arra az *Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé* [91] című cikk szerzői rámutatnak – az EU sajátos jogalkotási rendszeréből fakad. Az EU-ban megalkotott meghatározásokat a megjelenésük időrendjében mutatom be. *A kritikus infrastruktúrák védelme a terrorizmus elleni küzdelemben* című EU Bizottsági közlemény szerint: *„A kritikus infrastruktúrákhoz azok a fizikai és információs technológiai berendezések és hálózatok, szolgáltatások és eszközök tartoznak, amelyek összeomlása vagy megsemmisítése súlyos következményekkel járhat a polgárok egészsége, védelme, biztonsága és gazdasági jóléte, illetve a tagállamok kormányainak hatékony működése szempontjából. A kritikus infrastruktúrák több gazdasági ágazatra kiterjednek, többek között a bankügyletekre és pénzügyekre, a szállításra és forgalmazásra, az energiaiparra, a közművekre, az egészségügyre, az élelmiszerellátásra és tájékoztatásra, valamint a kulcsfontosságú állami szolgáltatásokra. Ezen ágazatok néhány kritikus eleme nem tartozik a szigorúan vett „infrastruktúra” fogalmába, de valójában olyan hálózatok vagy ellátási láncok, amelyek valamely alapvető termék vagy szolgáltatás biztosítását támogatják. Például a jelentős városi térségek élelmiszer- vagy vízellátása néhány kulcsfontosságú létesítménytől függ, ugyanakkor a termelők, feldolgozók, gyártók, forgalmazók és kiskereskedők összetett hálózata is szükséges az ellátás biztosításához.”* [30]

Az EU Bizottság *Zöld könyv a kritikus infrastruktúrák védelmére vonatkozó európai programról* című anyaga a kritikus infrastruktúrát a következőképpen határozza meg: *„A kritikus infrastruktúra magába foglalja azokat a fizikai erőforrásokat, szolgáltatásokat és információtechnológiai berendezéseket, hálózatokat és infrastruktúrákat, melyek összeomlása vagy megsemmisítése súlyos következményekkel járna a polgárok egészségére, biztonságára, védelmére vagy gazdasági jólétére, illetve a kormányzat hatékony működésére,”* [100].

Másként, rövidebben, de ugyanakkor többértelműen fogalmaz *Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről* szóló tanácsi irányelv: *„ ‘Kritikus infrastruktúra’: olyan eszközök, illetve azok részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, ideértve*

az ellátási láncot, az egészségügyet, a biztonságot, valamint az emberek gazdasági és társadalmi jólétét is" [28].

Ez kritikus infrastruktúra meghatározás további meghatározásokat követel, mert például *„A 'társadalmi feladat' és az 'ellátási lánc' fogalmak, illetve azok rendeltetése is tisztázatlan marad"* [91].

Ugyanez a javaslat az *európai kritikus infrastruktúra* fogalmát is definiálja: *„olyan kritikus infrastruktúra, amelynek megzavarása vagy megsemmisítése két vagy több tagállamot is jelentősen érintene, illetve csak egyetlen tagállamot érintene, de a kritikus infrastruktúra egy másik tagállamban van. Ide tartoznak azok a hatások is, amelyek az egyéb típusú infrastruktúrákkal fennálló, ágazatokon átnyúló szoros kapcsolatokból erednek"* [28].

Ez a megfogalmazás már a kritikus infrastruktúrák egy magasabb, szövetségi szintjét határozza meg. A fenti definíciós eltérések, a megfogalmazás egyre *lazábbá*, megengedőbbé válása arra utal, hogy az EU nem kívánja tagállamait korlátozni a kritikus infrastruktúrák kiválasztása során a túl szigorú és szabatos meghatározással. Ez célravezető az olyan országok esetében, ahol a témát komolyan feldolgozzák, és annak eredményeként pontos nemzeti kritikus infrastruktúra meghatározás születik, nem célravezető viszont azokban az országokban, ahol a védelem igénye nem belső felismerésből fakad, hanem *szükséges rossz*, amit a szövetségi rendszer *kényszerít ki.*

A kritikus infrastruktúrák védelme a terrorizmus elleni küzdelemben című EU Bizottsági közleménye [30] a kritikus infrastruktúra elemei közé az alábbi kilenc ágazatot (szektort) sorolja:

1. energiaipari létesítmények és hálózatok (pl. villamosenergia-, kőolaj- és földgáztermelés, tárolók és finomítók, szállító- és elosztóhálózat);
2. tájékoztatás és információs technológia (pl. távközlés, műsorszolgáltató rendszerek, szoftver, hardver és hálózatok, az internet is);
3. pénzügyek (pl. bankügyletek, értékpapír és befektetés);
4. egészségügy (pl. kórházak, egészségügyi és vérellátó létesítmények, laboratóriumok és gyógyszerellátók, felkutatás és mentés, sürgősségi ellátás);
5. élelmiszer (pl. biztonság, termelési eszközök, nagykereskedelmi forgalmazás és élelmiszeripar);
6. vízellátás (pl. gátak, víztárolás, -kezelés és -hálózatok);
7. közlekedés (pl. repülőterek, kikötők, intermodális létesítmények, vasúti és anyagszállítási hálózatok, forgalomirányító rendszerek);

8. veszélyes anyagok előállítása, tárolása és szállítása (pl. vegyi, biológiai, radioaktív és nukleáris anyagok);
9. állami infrastruktúrák (pl. létfontosságú szolgáltatások, berendezések, információs hálózatok, eszközök és jelentős nemzeti helyek és műemlékek).

Jól érzékelhető, hogy a felsorolt kritikus infrastruktúrák több gazdasági ágazatra kiterjednek, némely ágazatnak azonban van néhány olyan *létfontosságú* eleme, amely ugyan nem igazán tartozik az infrastruktúra szigorúan vett fogalmába, de valójában olyan hálózatok vagy kiszolgálórendszerek, melyek létfontosságú termék vagy szolgáltatás biztosítását támogatják, ezért a kritikus infrastruktúrához tartozónak tekintjük.

Az EU Bizottság *Zöld könyv a kritikus infrastruktúrák védelmére vonatkozó európai programról* című anyaga [100] a kritikus infrastruktúrákat már 11 ágazatba sorolja és megadja ezen ágazatok 37 alágazatát, ide értve termékeket vagy szolgáltatásokat is (1. táblázat).

1. táblázat – A kritikus infrastruktúra javasolt felsorolása [100]

Ágazat	Alágazat
I. Energia	1. kőolaj- és földgáz-kitermelés, finomítás, feldolgozás és tárolás, ideértve a csővezetékeket; 2. villamosenergia-termelés; 3. kőolaj-, földgáz- és villamosenergia-szállítás; 4. kőolaj-, földgáz- és villamosenergia-elosztás
II. Információs és kommunikációs technológiák, IKT	5. információs rendszerek és hálózatok védelme 6. műszerautomatizálási és felügyeleti rendszerek (SCADA stb.) 7. internet 8. vezetékes távközlési szolgáltatások 9. mobil távközlési szolgáltatások 10. rádiótávközlés és navigáció 11. műholdas távközlés 12. műsorszórás
III. Víz	13. ivóvíz szolgáltatás 14. vízminőség ellenőrzés 15. a vízmennyiség figyelemmel kísérése és ellenőrzése
IV. Élelmiszer	16. élelmiszer előállítás és élelmiszer-biztonság
V. Egészségügy	17. orvosi és kórházi ellátás 18. gyógyszerek, szérumok, oltóanyagok és gyógyászati eszközök 19. biológiai laboratóriumok és biológiai hatóanyagok
VI. Pénzügy	20. fizetési (elszámolási) szolgáltatások/ fizetési (elszámolási) rendszerek (magán) 21. kormányzati pénzügyi megbízatás
VII. Köz- és jogrend, közbiztonság	22. a köz- és jogrend, a közbiztonság fenntartása 23. igazságszolgáltatás és büntetés-végrehajtás

Ágazat	Alágazat
VIII. Közigazgatás	24. kormányzati feladatok 25. fegyveres erők 26. közigazgatási szolgáltatások 27. segélyszolgálatok 28. postai és futárszolgálatok
IX. Közlekedés	29. közúti közlekedés 30. vasúti közlekedés 31. légi forgalom 32. belvízi közlekedés 33. óceáni és tenger-melléki hajózás
X. Vegy- és nukleáris ipar	34. vegyi és nukleáris anyagok előállítása és tárolása/feldolgozása 35. veszélyes (vegyi) anyagok csővezetékei
XI. Világűr és kutatások	36. világűr 37. kutatások

Véleményem szerint ez a felsorolás több nehezen értelmezhető pontot tartalmaz. Például az *5. információs rendszerek és hálózatok védelme* alatt azt kellene érteni, hogy nem az információs rendszerek és hálózatok, hanem csak azok védelme tartozik a kritikus infrastruktúrához? További zavaró, hogy a *VIII. Közigazgatás* (Civil administration) ágazatban *25. a fegyveres erők*, valamint *28. a postai és futárszolgálatok* is szerepelnek.

Megítélésem szerint további problémát jelent, hogy *Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről* szóló tanácsi irányelv [28] már másik 11 – a Zöld Könyvben leírtakkal sem tartalmában, sem sorrendjében nem egyező – ágazatot és annak 29 alágazatát adja meg (2. táblázat).

2. táblázat – A kritikus infrastrukturális ágazatok listája [28]

Ágazat	Alágazat
I. Energia	1. olaj- és gáztermelés, finomítás, feldolgozás, tárolás és vezetékes elosztás 2. villamosenergia-termelés és –továbbítás
II. Nukleáris ipar	3. nukleáris anyagok előállítása és tárolása/feldolgozása
III. Információs és kommunikációs technológiák (IKT)	4. információs rendszerek és hálózatok 5. műszerautomatizálási és felügyeleti rendszerek (SCADA stb.) 6. internet 7. vezetékes távközlési szolgáltatások 8. mobil távközlési szolgáltatások 9. rádiós távközlés és navigáció 10. műholdas távközlés 11. műsorszórás
IV. Víz	12. ivóvíz szolgáltatás 13. vízminőség ellenőrzés 14. a vízmennyiség figyelemmel kísérése és ellenőrzése

Ágazat	Alágazat
V. Élelmiszer	15. élelmiszer-ellátás és élelmiszer-biztonság
VI. Egészségügy	16. orvosi és kórházi ellátás 17. gyógyszerek, szérumok és oltóanyagok 18. biológiai laboratóriumok és biológiai hatóanyagok
VII. Pénzügy	19. fizetési, valamint értékpapírklíring- és elszámolási infrastruktúrák és rendszerek 20. szabályozott piacok
VIII. Közlekedés	21. közúti közlekedés 22. vasúti közlekedés 23. légi közlekedés 24. belvízi közlekedés 25. óceáni és tenger-melléki hajózás
IX. Vegyipar	26. vegyi anyagok előállítása és tárolása/feldolgozása 27. veszélyes (vegyi) anyagok vezetékes elvezetése
X. Világűr	28. világűr
XI. Kutatóberendezések	29. kutatóberendezések

Véleményem szerint a korábbi lista szűkítésének, azaz a *VII. Köz- és jogrend, közbiztonság* és a *VIII. Közigazgatás ágazat* kikerülésének egyik legjelentősebb oka, hogy ezek a területek belügyek, nemzeti hatáskörbe tartoznak, és így az EU a védelmükkel kapcsolatban nem intézkedhet.

1.3.2. A NATO KRITIKUS INFRASTRUKTÚRA MEGHATÁROZÁSA

A NATO a kritikus infrastruktúrák védelmét, **mint a polgári védelem szerves részét** definiálja. [78] Ezen a területen a NATO különös figyelmet szentel az EU-val történő együttműködésre.

A kritikus infrastruktúra meghatározását a NATO Polgári Védelmi Bizottság[24] dolgozta ki, amely a következő: „*A kritikus infrastruktúra azokat a létesítményeket, szolgáltatásokat és információrendszereket jelenti, amelyek olyan létfontosságúak a nemzetek számára, hogy működésképtelenné válásuknak vagy megsemmisülésüknek gyengítő hatása lenne a nemzet biztonságára, a nemzetgazdaságra, a közegészségre és közbiztonságra és a kormány hatékony működésére”* [39].

A fenti meghatározás az Amerikai Egyesült Államok kritikus infrastruktúra meghatározásával (lásd 1.3.4. pont) van összhangban, szinte csak fogalmazásbeli eltéréssel.

[24] Civil Protection Committee (CPC)

Megítélésem szerint a NATO ezzel a kérdéssel egyre többet foglalkozik. Ennek egyik oka, hogy a szövetséges országok infrastruktúráit, ezek között számos kritikus infrastruktúrát a szövetség is használ, használna rendkívüli helyzetekben is.

Véleményem szerint a NATO a kritikus infrastruktúrák védelme tekintetében nagyon szoros, a szövetség eddigi gyakorlatában példátlan együttműködést kíván kialakítani az Európai Unióval a közös célok és azonos megoldások elve miatt.

1.3.3. AZ EGYESÜLT KIRÁLYSÁG KRITIKUS INFRASTRUKTÚRA MEGHATÁROZÁSA

Az Egyesült Királyság Nemzeti Infrastruktúra Biztonsági Koordinációs Központ[25] a következőképpen definiálta a nemzet számára kritikus infrastruktúra fogalmát: „*Létfontosságú nemzeti infrastruktúra mindaz az eszköz, szolgáltatás és rendszer, amely az Egyesült Királyság gazdasági, politikai és társadalmi életét támogatja, s amelyek fontossága olyan mérvű, hogy teljes vagy részleges hiánya vagy veszélyeztetettsége tömeges halált okoz, a nemzetgazdaságban súlyos hatással bír, a közösség részére egyéb súlyos társadalmi következménnyel jár, azonnal hatást okoz a Kormánynak.”* [55]

A fentiek alapján meghatározható kritikus infrastruktúrákat 9 független szektorba csoportosították:

1. bank és pénzügyi szektor;
2. energia;
3. élelmezés;
4. kommunikáció;
5. kormányzati és közigazgatási szolgáltatások;
6. készenléti szolgáltatás (pl.: tűzoltóság);
7. közbiztonság;
8. közlekedés;
9. vízellátás.

Véleményem szerint a fenti felsorolás a vegy- és nukleáris ipar kihagyásával azonos az Európai Unió Zöld Könyvében azonosított ágazatokéval.

[25] National Infrastructure Security Co-ordination Centre (NISCC)

1.3.4. AZ USA KRITIKUS INFRASTRUKTÚRA MEGHATÁROZÁSA

A kritikus infrastruktúrával kapcsolatos legkorábbi és legkiforrottabb munkák az Amerikai Egyesült Államokban születtek. Az Egyesült Államok *Kritikus Infrastruktúrák védelméről szóló* 2001-es törvény, az úgynevezett *Patriot Act* [99] meghatározása szerint a kritikus infrastruktúrához *„azok a fizikai és virtuális rendszerek, eszközök tartoznak, melyek olyannyira létfontosságúak az Egyesül Államok számára, hogy e rendszerek és eszközök működésképtelensége vagy megsemmisülése gyengítené a védelmet, a nemzeti gazdaság biztonságát, a nemzeti közegészséget és biztonságot vagy mindezek kombinációját."*

Az Amerikai Egyesült Államokban már 1997-ben, egy a Clinton elnök által felkért bizottság nyolc kulcsfontosságú infrastruktúrát nevesített, amelyek kritikusak lehetnek az ország szempontjából [32]:

1. telekommunikáció;
2. elektromos energia;
3. kőolaj- és földgáztárolás, valamint szállítás;
4. bank és pénzügy;
5. szállítás;
6. vízellátás;
7. segélyszolgálatok (ideértve a mentőket, a rendőrséget, a tűzoltókat és műszaki mentést);
8. közigazgatási szolgáltatások.

Ez a felsorolás mai szemmel koránt sem tekinthető teljesnek, és a felelősségek megosztása is komoly gondokat okozott, ezért a 2001. szeptember 11-i terrortámadást[26] követően e kérdéseket újra áttekintették és a legmagasabb szinten szabályozták. *A Kritikus Infrastruktúra Azonosításáról, Besorolásáról és Védelméről* szóló *HSDP-7 Belbiztonsági Elnöki Iránymutatás*[27] [49] a koordinációért felelős személyek és szervezetek kijelölésével egyidejűleg az alábbiak szerint határozta meg a védelmet igénylő nemzeti infrastrukturális szektorokat és kulcseszközöket:

A belbiztonsági miniszter közvetlen felelősségében:

[26] 2001. szeptember 11-én az *al-Kaida* arab terrorszervezet által elkövetett támadás New Yorkban és Washingtonban.

[27] Homeland Security Presidential Directive (HSDP)

1. informatika;
2. telekommunikáció;
3. kémiai ipar;
4. közlekedési rendszerek, ideértve a tömegközlekedést, repülést, folyami és tenger hajózást, vasúti és csővezeték rendszereket.
5. segélyszolgálatok;
6. postai és áruszállítás;

A Belbiztonsági Minisztérium közvetlen irányításával szakminisztériumok felelősségében:

7. gátak;
8. közigazgatási létesítmények;
9. kereskedelmi létesítmények;

Az egyes szakminisztériumok és hivatalok hatáskörében:

10. mezőgazdaság, élelmiszer (hús-, baromfi-, tojástermékek);
11. közegészségügy, egészségügyi ellátás és élelmiszer (nem hús-, baromfi-, tojástermékek);
12. ivóvíz és vízellátó rendszerek;
13. energia, ideértve a kőolaj és földgáz termékfinomítást, tárolást és forgalmazást, az elektromos energiát, kivéve a kereskedelmi nukleáris erőmű berendezéseket;
14. bank és pénzügy;
15. nemzeti emlékhelyek és szobrok;
16. védelmi ipari bázis;
17. kereskedelmi nukleáris reaktorok az elektromos áram előállítására és fejlesztést, tesztelést és gyakorlást szolgáló nem teljesítmény nukleáris reaktorok, a nukleáris anyagok a gyógyászatban, iparban és az akadémiai környezetekben és a nukleáris üzemanyag-gyártás létesítményei, valamint a nukleáris anyag- és hulladékszállítás, tárolás és kezelés.

A fentiekben az elsődlegesen a nemzet biztonságának és gazdaságának működése szempontjából szükséges infrastruktúra lista olyan speciális eszközökkel is bővült, amelyek a közösségek szempontjából lényegesek. Ezek alapvetően nem kritikus elemei a nemzet védelmének vagy gazdaságának, de társadalmi szempontból *kritikusak* (pl. nemzeti emlékművek, képek). A fentiek miatt külön fogalmat alkotottak az eredetileg a kritikus infrastruktúrába nem tartozó olyan egyéni célpontokra, melyek „*megsemmisítése nem*

veszélyeztetne létfontosságú rendszereket, azonban helyi katasztrófát okozna, vagy nagymértékben rongálná a nemzeti morált és bizalmat". Ilyen ún. kulcslétesítmények például a nemzeti emlékhelyek, szobrok, vagy a helyi közösségek számára értékes iskolák, bíróságok vagy hidak. Ezen eszközök védelme elsősorban tagállami vagy helyi szintű, de a nemzeti stratégia szövetségi segítségnyújtással támogatja a védelmüket.

Véleményem szerint ez egy nagyon alaposan átgondolt sok, talán túl sok szempontot is figyelembe vevő, de nagyon részletes lista. A felelős személyek, szervezetek kijelölése megítélésem szerint a korábbi rossz tapasztalatokból következett be. Az is megállapítható, hogy a társadalmi-politikai szempontok figyelembe vétele csak a 2001. szeptember 11-i terrortámadás után következett be.

1.3.5. A MAGYAR KÖZTÁRSASÁG KRITIKUS INFRASTRUKTÚRA MEGHATÁROZÁSA

Hazánkban a kritikus infrastruktúrák védelmével kapcsolatos egységes, definíciókat is tartalmazó dokumentum nyilvánosan nem érhető el. Az egyes jogszabályok is csak a *minimálisan szükséges* mértékben foglalkoznak e kérdéssel. A kritikus infrastruktúra meghatározását megadja *Az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségéről szóló 27/2004. (X.6.) IHM rendelet,* de ez csak e rendelet vonatkozásában határozza meg a kritikus infrastruktúra definícióját.. A rendelet szerint kritikus infrastruktúra „*mindazon létesítmények, szolgáltatások – beleértve az elektronikus hírközlési és informatikai rendszereket – melyek működésképtelenné válása vagy megsemmisülése egyenként és együttesen jelentősen befolyásolhatja a nemzet biztonságát, az állampolgárok élet- és vagyonbiztonságát, a nemzetgazdaság és a közszolgáltatók működését"*. [10] Ez a meghatározás elfogadható, de az informatikai és hírközlési miniszter jogköre nem terjedt ki védelmi kérdésekben való állásfoglalásra, így rendelete a védelemben érintett körnek csak egy részére vonatkozik, továbbá a fogalom definiálása ellenére nyitottan hagyja azt a kérdést, hogy konkrétan mely infrastruktúrák tartoznak a meghatározás során a hatálya alá. A kérdés ilyen kezelése zavart okozhat a közigazgatásban.

A terrorizmus elleni küzdelem aktuális feladatairól szóló *2112/2004. (V.7.) Korm. határozat* a kritikus infrastruktúra következő szektorait említi elsősorban.

1. energiaellátás;
2. közművesítés;
3. közlekedés;
4. szállítás;
5. távközlés;
6. elektronikus adatforgalom;
7. informatikai hálózat;
8. a bankrendszer;
9. a szolgáltatások;
10. média;
11. ivóvíz és élelmiszer alapellátás;
12. egészségügyi biztosítás.

A fenti felsorolás számos vonatkozásában eltér mind az EU, mind más államok által meghatározottaktól. Így például, nem tartalmazza a közigazgatást, a védelmi és készenléti jellegű szervezeteket, úgymint rendőrséget, vámőrséget, honvédséget, illetve a segélyszolgálatokat[28].

A felsorolásról árulkodik, hogy hevenyészve, meggondolatlanul állították össze. Megjelenik benne az informatikai hálózat mellett az elektronikus adatforgalom (?), hiányzik ugyanakkor a távközlés. A közművesítés kifejezést a közművek (villany-, gáz-, víz- és csatorna-, telefonhálózatok) kiépítésére használjuk, a helyes a közművek lett volna. Az egészségügyi biztosítás a katonai nyelvezetben ismert, de a civilszféra könnyen összekeveri az egészségbiztosítással, aminek a működtetése nem létfontosságú, szemben a nehezen nélkülözhető egészségügyi ellátással.

A *Nemzeti Biztonsági Stratégiában* [6] a biztonsági környezet elemzése, az érdekek megfogalmazása, valamint a célok, feladatok és eszközök, meghatározása tükrözi a NATO-tagságból és EU-csatlakozásból adódó integrációs teendőket, de sem a kritikus infrastruktúra fogalmát, sem az abba tartozó infrastruktúrákat nem határozza meg.

Véleményem szerint a fentiek miatt szükséges a Magyar Köztársaság kritikus infrastruktúráinak pontos meghatározása!

[28] Segélyszolgálat alatt a mentő-, tűzoltó- és más vészhelyzeti segítségnyújtó szervezetek és szolgáltatásait értem.

1.4. A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK MEGHATÁROZÁSA KÜLÖNBÖZŐ ORSZÁGOKBAN ÉS SZERVEZETEKBEN

A kritikus infrastruktúra elemei között valamennyi, az előző pontban bemutatott esetben megjelentek az infokommunikációs technológiák. Az infokommunikációs technológiák önálló megjelenésén túl figyelemre méltó az a tény, hogy napjainkban szinte valamennyi kritikusnak minősített, vagy annak minősíthető infrastruktúra nemcsak használja az infokommunikációs technológiákat, hanem egyre erősebben függ is ezektől. Az infokommunikációs technológiáktól függ az egyes kritikus infrastruktúra elemek működése és függ a kritikus infrastruktúra elemeinek együttműködése is, más szóval az infokommunikációs technológiáktól való függőség olyan mértékű, hogy azok összeomlása vagy megsemmisülése súlyos következményekkel járhat nem csak az adott infrastruktúra szempontjából, hanem más kritikus infrastruktúrákra nézve is. A kritikus információs infrastruktúra egészére nézve az egyes infrastruktúra elemek infokommunikációs technológiái egy belső kritikus infrastruktúrát jelentenek.

Kijelenthetjük, hogy az infrastruktúrák között kölcsönös függőség áll fenn. A támogató információs infrastruktúrákon[29] keresztül az információs társadalom funkcionális információs infrastruktúráinak[30] működését károsan lehet befolyásolni (zavarni, korlátozni, megszüntetni), azon keresztül pedig:

- az információs társadalom információs és vezetési működési rendjére (minőségére, harmóniájára, dinamikus egyensúlyára);
- vezetési rendszerére (a vezetés integrációjára, annak szilárdságára és minőségére);
- a vezetés struktúrájára (szervezettségi fokára);
- a belső és külső kommunikációra és végezetül
- az adott szervezet operatív vezethetőségére lehet igen komoly, negatív hatást gyakorolni.[47]

[29] A támogató információs infrastruktúrák biztosítják a funkcionális információs infrastruktúrák működéséhez a támogató hátteret. [48]

[30] A funkcionális információs infrastruktúrák biztosítják a társadalom működéséhez az információk megszerzését, előállítását, továbbítását, feldolgozását és felhasználását, azaz közreműködnek minden alapvető társadalmi feladat – funkció – ellátásában. [48]

„Szinte minden fajta kritikus infrastruktúrát különböző szintű és rendeltetésű infokommunikációs rendszerek vezérelnek, irányítanak és ellenőriznek. Így tehát egy ország információtechnológiára alapozott infrastruktúrája joggal nevezhető a társadalom idegrendszerének, és ennek következtében az információs infrastruktúrák, illetve azok részei is a kritikus infrastruktúrák közé sorolandók. E megállapítás szerint, pl. egy ország nyilvános mobil távközlő hálózatai, mint önmagukban is kritikus infrastruktúrák, egyben kritikus információs infrastruktúráknak is minősülnek, illetve pl. az energiaellátó rendszert irányító, vezérlő számítógép-hálózat is ez utóbbiak közé sorolandó." [46]

A kritikus információs infrastruktúra fogalmi tisztázásában igen jelentős szerepet kap az Európai Bizottság által 2005 novemberében közreadott *Zöld Könyv a kritikus infrastruktúrák védelem európai programjáról.* E fontos okmány nemcsak a kritikus infrastruktúrát, hanem a kritikus információs infrastruktúrát is meghatározza. A dokumentum ajánlotta meghatározás a következő:

„A kritikus információs infrastruktúra *azokat az infokommunikációs rendszereket jelenti, amelyek önmagukban is kritikus infrastruktúra elemek, vagy lényegesek az infrastruktúra elemei működésének szempontjából (távközlés, számítógépek és szoftver, internet, műholdak stb.)"* [100]

E dokumentum szerint a kritikus információs infrastruktúrák védelme a „*tulajdonosok, üzemeltetők, gyártók és használók, valamint a hatóságok programjai és tevékenységei, melyek célja fenntartani a kritikus információs infrastruktúra teljesítményét meghibásodás, támadás vagy baleset esetén a meghatározott minimális szolgáltatási szint felett, illetve minimálisra csökkenteni a helyreállításhoz szükséges időt, valamint a károkat."*

A kritikus információs infrastruktúrák védelme tehát ágazatközi jelenség, nem korlátozódik egyes konkrét ágazatokra. A kritikus információs infrastruktúrák védelmét szorosan koordinálni kell magával a kritikus infrastruktúrák védelemmel.

A fogalom-meghatározások után felsorolt infrastruktúra elemek adott esetben nem is mindig tekinthetők az infrastruktúra részének, vagy pedig nem az egészük tekinthető kritikusnak.

Az Egyesült Királyságban a társadalomra jellemző, hogy a különböző szervezetek és cégek mindennapos tevékenysége erősen kötődik a számítógépekhez és az ahhoz kapcsolódó elektronikus technológiákhoz, mely által elektronikus támadással szemben fokozottan sérülékennyé minősíthetők. Számos rendszerük már az internethez kapcsolódik, mely az üzleti hatékonyság mellett a közvetlen támadási útvonalat is biztosítja a lehetséges elkövetők számára.

Az Egyesült Királyságban a kritikus nemzeti infrastruktúra[31] védelmének kiemelt területeként kezelik az infokommunikációs rendszerek védelmét. A kritikus információs infrastruktúrák védelme alatt elsősorban a kritikus nemzeti infrastruktúra elemeinél az információbiztonsági, az infokommunikációs biztonsági szabványok és ajánlások használatát szorgalmazzák. [27], [87]

Ausztriában napjainkban az államra, a társadalomra és az egyénre vonatkozó veszélyforrásokat a politikából, a gazdaságból, a hadügyből, magából a társadalomból, a környezetből, a kultúrából és a vallásból, valamint az információtechnológiából eredeztetik. Megállapítják, hogy az információtechnológia új biztonsági dimenzióként jelent meg az elmúlt időben, amely saját területet igényel a biztonság általános kérdéskörén belül, mivel számos kapcsolata – adott esetben komoly hatása – van a biztonság egyéb aspektusaival.

Mindezidáig azonban Ausztriának nincs egységes és elfogadott definíciója a kritikus infrastruktúrákra. Ugyanakkor abban egyetértés van, hogy egy olyan kis ország, mint Ausztria különösen sebezhető az információs infrastruktúráin keresztül. Ez a sebezhetőség igaz a polgári és a katonai rendszerekre, valamint egyre növekvő mértékben az üzleti és ipari életre.

A közeljövőre nézve az a legvalószínűbb, hogy az ország, mint Európai Uniós tagállam, átveszi az EU kritikus infrastruktúra meghatározását. [56]

Az Amerikai Egyesült Államokban már 1997-ben egy a Clinton elnök által felkért bizottság meghatározta azokat a kulcsfontosságú rendszereket, amelyek kritikusak lehetnek az ország szempontjából [32].

Az Egyesült Államok esetében az infokommunikációs biztonság szinte minden aspektusban érinti a kritikus infrastruktúrák védelmét. A legtöbb amerikai vállalkozás már nem képes az infokommunikációs rendszert a fizikai működésétől elválasztani, mert azok annyira összekapcsolódtak. *„A cybertér a nemzeti infrastruktúránk idegrendszere – ellenőrző rendszere országunknak. A cybertér száz meg százezer számítógép, szerver, router, switch, és optikai kábel összekapcsolódásából áll, mely kritikus infrastruktúráinkat működteti. Így tehát a cybertér egészséges működése is létfontosságú gazdaságunk és nemzeti biztonságunk számára”* [98]

Hazánkban a kritikus információs infrastruktúrák védelmével kapcsolatos egységes, definíciókat is tartalmazó dokumentum nyilvánosan nem érhető el. Egyedül a már említett *Az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének*

[31] Critical National Infrastructure (CNI)

létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségéről szóló 27/2004. (X.6.) IHM rendelet intézkedik nemzeti szinten az *elektronikus védelemről*, a *hálózatbiztonságról* az ügyeleti rendszer kapcsán, de csaka minisztérium jog- és hatáskörében, így nem határozza meg a védelem pontos körét.

Mindezek alapján azt a következtetést vonom le, hogy a kritikus infrastruktúra elemnek minősített **infokommunikációs technológia** és a kritikus infrastruktúra elemek **infokommunikációs technológiája együttesen** alkotják a **kritikus információs infrastruktúrát**.

Összegezve a megvizsgált szervezetek és országok kritikus információs infrastruktúra meghatározásait és azokat a területeket, amelyeket ide sorolnak, megállapítható, hogy **kritikus információs infrastruktúra körébe a következő elemek (rendszerek) tartozhatnak:**

- vezetékes, mobil és műholdas kommunikációs hálózatok;
- kormányzati és önkormányzati számítógép-hálózatok;
- védelmi szféra riasztási, távközlési, számítógép-hálózatai;
- energiaellátó rendszerek rendszerirányító számítógép-hálózatai;
- közlekedés szervezés és irányítás számítógép-hálózatai és kommunikációs rendszere;
- pénzügyi-gazdasági rendszer számítógép-hálózatai;
- egészségügyi rendszer számítógép-hálózatai és kommunikációs rendszere.

1.5. JAVASLAT A MAGYAR KÖZTÁRSASÁG KRITIKUS INFRASTRUKTÚRA ÉS KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA MEGHATÁROZÁSAIRA

Az előzőekben láthattuk, hogy hazánknak nincs egyértelműen meghatározott kritikus infrastruktúra és kritikus információs infrastruktúra fogalma, illetve a meglévő meghatározások nem fedik le tartalmukban teljesen azokat a területeket, szektorokat és elemeket, amelyek a kritikus kategóriába tartoznak.

A kritikus infrastruktúra meghatározásait és a hazai helyzetet áttanulmányozva arra a következtetésre jutottam, hogy a kritikus infrastruktúra meghatározását hazánkban nem szabad sem túl szélesre, megengedőre, sem nagyon leszűkítőre venni, mert ezekben az esetekben nagyon sok utólagos elemzést és értelmezés vonhat maga után, megnehezítve az érdemi munkát. Az infrastruktúrák körét – az USA mintáját elfogadva – bővítettem a jelentős morális kár lehetőségét hordozó létesítményekkel.

Javaslatom szerint a hazai **kritikus infrastruktúra fogalom a következő**:
Azon létesítmények, eszközök vagy szolgáltatások, amelyek működésképtelenné válása, vagy megsemmisülése a nemzet biztonságát, a nemzetgazdaságot, a közbiztonságot, a közegészségügyet vagy a kormány hatékony működését gyengítené, továbbá azon létesítmények, eszközök és szolgáltatások, amelyek megsemmisülése a nemzeti morált vagy a nemzet biztonságába, a nemzetgazdaságba, vagy a közbiztonságba vetett bizalmat jelentősen csökkentené.

Javaslatom szerint a hazai **kritikus információs infrastruktúra fogalom a következő**:
Azon az infokommunikációs létesítmények, eszközök vagy szolgáltatások, amelyek önmagukban is kritikus infrastruktúra elemek, továbbá a kritikus infrastruktúra elemeinek azon infokommunikációs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása, vagy megsemmisülése a kritikus infrastruktúrák működésképességét jelentősen csökkentené.

A fenti definíciók, a nemzetközi minták és a hazai helyzet elemzése alapján **arra a következtetésre jutottam**, hogy a kritikus infrastruktúra elemeinek meghatározásánál – az EU Zöld Könyvét alapul véve – egy minél szélesebb körű felsorolást kell megadni. Az elemek felsorolásnál **célszerűnek láttam** a **felelősségi körök kijelölését**, mert ennek hiányában nem érzem biztosítottnak a védelem maradéktalan végrehajtását, mivel a hazai viszonyokra különösen jellemző, hogy ha nincs jogszabályban megnevezett, konkrét felelős (irányító és ellenőrző) akkor a feladatot minden érintett elkerüli, és annak végrehajtásához nem lesz koordináló, információt szolgáltató, a végrehajtást ellenőrző, számon kérhető személy.

A Magyar Köztársaság kritikus infrastruktúráihoz tartozó alágazatokat az alábbiak szerint javaslom meghatározni (az alkalmazott számozás nem fontossági vagy prioritási rendet mutat)**:**

A Miniszterelnöki Hivatal vezető miniszter közvetlen koordinációjával a szakminiszter irányításában:

1. Informatikai rendszerek és hálózatok;
2. Automatizálási, vezérlési és ellenőrzési rendszerek (SCADA, távmérő, távérzékelő és telemetriai rendszerek, stb.);
3. Internet szolgáltatás (infrastruktúra is);
4. Vezetékes távközlési szolgáltatások;

5. Mobil távközlési szolgáltatások;
6. Rádiós távközlés és navigáció;
7. Műholdas távközlés;
8. Műsorszórás;
9. Közigazgatási informatika és kommunikáció;
10. Közúti közlekedés;
11. Vasúti közlekedés;
12. Légi közlekedés;
13. Belvízi közlekedés;
14. Áruszállítás és logisztikai központok;
15. Ivóvíz szolgáltatás;
16. Segélyszolgálatok (mentők, tűzoltók, polgári védelem);
17. Védelmi létesítmények és eszközök;
18. Közigazgatási létesítmények, eszközök és szolgáltatások;

A gazdasági és közlekedési miniszter felelősségében (irányításában):

19. Kőolaj- és földgáztermelés, finomítás, feldolgozás, tárolás és vezetékes elosztás;
20. Villamosenergia-termelés és -továbbítás;
21. Postai szolgáltatások;

A gazdasági és közlekedési miniszter felelősségében, az Országos Katasztrófavédelmi Főigazgatóval együttműködve:

22. Vegyi anyagok előállítása, tárolása és feldolgozása;
23. Veszélyes anyagok (hulladékok is) kezelése, tárolása és szállítása;
24. Nukleáris anyagok (hulladékok is) előállítása, tárolása, feldolgozása é szállítása;
25. Nukleáris anyagok a gyógyászatban, iparban és az akadémiai környezetekben;

A környezetvédelmi és vízügyi miniszter felelősségében (irányításában):

26. Vízminőség ellenőrzés;
27. Szennyvíztisztítás;
28. Gátak és belvízelvezetés, a vízmennyiség figyelemmel kísérése és ellenőrzése;

A földművelésügyi és vidékfejlesztési miniszter felelősségében (irányításában):

29. Élelmiszer-termelés;
30. Élelmiszer-ellátás;
31. Élelmiszer-biztonság;

Az egészségügyi miniszter felelősségében (irányításában):

32. Rendelőintézeti (háziorvosi) és kórházi ellátás;
33. Oltóanyag és gyógyszergyártás;
34. Egészségügyi tartalékok és vérkészletek;
35. Gyógyszerek, szérumok és oltóanyagok;
36. Biológiai laboratóriumok és biológiai hatóanyagok;

A pénzügyminiszter felelősségében (irányításában):

37. Pénz- és hitelintézetek;
38. Fizetési, valamint értékpapírklíring- és elszámolási infrastruktúrák és rendszerek;
39. Szabályozott piacok (pénz- és árutőzsde);

Az igazságügyi és rendészeti miniszter felelősségében (irányításában):

40. Igazságszolgáltatás;
41. Rendvédelmi szervek infrastruktúrái;
42. Nemzeti szimbólumok.

A fenti felsorolásban törekedtem a teljes körűségre, amely a konkrét kritikus infrastruktúra elemek besorolásakor megengedi, hogy valamely fent megjelölt alágazatnak csak egyes elemei kerüljenek be a védelemre kijelölt elemek közé, de mindenképp vizsgálni kell az adott alágazatot és nem merül fel a *jogosulatlan kiterjesztés* kérdése.

A korábbiakban megállapítottam, hogy a fegyveres erőket, a fegyveres erők infrastruktúráit általában nem sorolják be a kritikus infrastruktúrák közé. A védelmi szféra kritikusnak minősített infrastruktúrái minden esetben összefüggenek a polgári- vagy a katasztrófavédelemmel. Ennek alapján a Magyar Honvédség tulajdonában, kezelésében lévő infrastruktúrákat nem soroltam a kritikus infrastruktúrák közé, mivel saját infrastruktúráinak védelme – a felkészüléstől a felderítésen keresztül az esetlegesen elszenvedett csapások utáni helyreállításig – az alapfeladatai közé tartozik.

Mindezeket figyelembe véve, a Magyar Köztársaság kritikus információs infrastruktúraihoz tartozó alágazatokat az alábbiak szerint javaslom meghatározni (az alkalmazott számozás nem fontossági vagy prioritási rendet mutat)**:**

1. Informatikai rendszerek és hálózatok;
2. Automatizálási, vezérlési és ellenőrzési rendszerek (SCADA, távmérő, távérzékelő és telemetriai rendszerek, stb.);
3. Internet szolgáltatás (infrastruktúra is);
4. Vezetékes távközlési szolgáltatások;
5. Mobil távközlési szolgáltatások;
6. Rádiós távközlés és navigáció;
7. Műholdas távközlés;
8. Műsorszórás;
9. Közigazgatási informatika és kommunikáció;
10. A kritikus infrastruktúrák létfontosságú infokommunikációs rendszerei.

KÖVETKEZTETÉSEK

Megvizsgáltam az Európai Unió, a NATO és több ország, köztük a Magyar Köztársaság kritikus infrastruktúra, kritikus információs infrastruktúra fogalmát, illetve elemeinek meghatározását. Megállapítottam, hogy a definíciók általánosságában lefedik egymást, a különbségek az országok eltérő fejlettségéből vagy gazdasági, illetve kulturális strukturáltságából, értékrendjéből, gondolkodás módjából fakadnak.

A fentiekből következik, hogy a kritikus infrastruktúra, kritikus információs infrastruktúra elemeinek jó meghatározásához **először a fogalomrendszert kell rögzíteni**. Az elemek meghatározása során nem alkalmazhatók szabadon más országok meghatározásai, mert **az egyes országok fejlettségét, gazdasági és kulturális strukturáltságát, értékrendjét, gondolkodásmódját is vizsgálni kell**. Az adott nemzet vonatkozásában **konkrétan kell meghatározni a kritikus infrastruktúra, kritikus információs infrastruktúra elemeit**.

Megállapítható, hogy valamennyi meghatározás kritikus infrastruktúraként tekint az infokommunikációs (informatikai és kommunikációs) rendszerekre. A kritikus információs infrastruktúra elemeinek meghatározása során az infokommunikációs rendszereket nagyon hasonló tartalommal sorolják a kritikus infrastruktúrába.

Elgondolásom, hogy a kritikus információs infrastruktúrák védelmében az intradependencia miatt a kritikus infrastruktúra **infokommunikációs rendszerei biztonságának megteremtése és fenntartása felértékelődik**, a védelem egyik alapvető elemévé válik.

A kritikus információs infrastruktúra tulajdoni viszonyai heterogének, dominál a magántulajdon. A tulajdonosoknak nem mindig egyértelmű érdeke a biztonság fokozása, mert annak költségei a nyereséget csökkentik[32], ezért a védelem megvalósításához kölcsönös előnyök biztosítása szükséges.

Megállapítottam, hogy a Magyar Köztársaság kritikus információs infrastruktúráinak meghatározásakor hatókör szempontjából az országra gyakorolt **hatás alapján** kell kijelölni a **kritikus információs infrastruktúrákat**. A nagyságrend figyelembe vétele során a jelentős hatású veszteségek a mérvadóak, de a közepes vagy mérsékelt hatás esetén vizsgálni kell annak időbeli hatását is. Amennyiben a hatás hosszabb távon fennmarad, például maradandó környezetkárosodás, a hatásában alacsonyabb nagyságrendű infrastruktúrák is a közepesek közé sorolandók.

Az inter- és intradependencia vizsgálata mind az infrastruktúrák besorolása, mind a védelmi intézkedések kialakítása során nagy jelentőséget kell, hogy kapjon, ezért – különösen a védelmi intézkedések kialakítása során – a vizsgálatnak egyaránt ki kell terjednie az infrastruktúrák interdependenciájára és intradependenciájára.

A tulajdonviszonyokra hazánkban a magántulajdon jellemző, amely felveti a pontos törvényi előírások szükségességén túl a kölcsönös érdekek keresését is.

Kutatásom során megállapítottam, hogy a fegyveres erőket, a fegyveres erők infrastruktúráit általában **nem sorolják** be a kritikus infrastruktúrák közé. A védelmi szféra kritikusnak minősített infrastruktúrái minden esetben összefüggenek a polgári védelemmel vagy a katasztrófavédelemmel. A fegyveres erők feladatai közé mindig és mindenhol bele tartozott saját infrastruktúráinak védelme, a felkészüléstől a felderítésen keresztül az esetlegesen elszenvedett csapások utáni helyreállításig. Ugyanakkor békeidőszakban nem lehet katonai feladat – védelmi célokat közvetlenül nem ellátó – polgári létesítmények védelme, szolgáltatások felügyelete. A NATO megoldásai, a kérdéssel foglalkozó bizottságai

[32] Tudatosítani kell, hogy az *elmaradt haszon az veszteség* gazdasági bölcsesség mintájára az *elmaradt kár az haszon* tétel is létezik, vagyis azt, hogy a kár az veszteség, és a meghatározható valószínűségű veszteség elkerülése haszonként fogható fel. Ebből egyenesen következik, hogy a potenciálisan bekövetkező károk elkerülésére tett intézkedés nem *pénzkidobás,* hanem olyan beruházás, amely azáltal hoz hasznot, hogy nem következik be a veszteség. [85]

helyzete is alátámasztják azt a véleményemet, hogy **a kritikus infrastruktúrák védelme nem katonai feladat**. Ettől függetlenül úgy ítélem meg, hogy a kritikus infrastruktúrák védelme területén a **fegyveres erőknek számos feladata van**. Az ország védelmi tevékenységének tervezése, koordinációja elképzelhetetlen a fegyveres erők részvétele nélkül, és ezen túlmenően a védelmi felkészülés irányításában, a felkészülésben és felkészítésben, különösen a kérdéskör tudományos kutatásában számos feladatban szükséges a bevonásuk.

E fejezetben mindezek alapján **meghatároztam a Magyar Köztársaság kritikus infrastruktúra fogalmát, a kritikus infrastruktúrák alágazatait és felelőseit,** valamint a **Magyar Köztársaság kritikus információs infrastruktúra fogalmát** és azok **alágazatait.**

2. FEJEZET
A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK FENYEGETETTSÉGE ÉS VÉDELME

2.1. A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK FENYEGETETTSÉGE

2.1.1. FENYEGETÉSEK A FIZIKAI DIMENZIÓBÓL

A következőkben néhány veszély típus látható, amelyek közvetlenül vagy közvetve képesek fenyegetést jelenteni az információs infrastruktúrák elemeire:

a.) Természeti katasztrófák
- vízkárok (közművek sérülése, árvíz, belvíz);
- geológiai katasztrófák (földrengés, talajsüllyedés);
- meteorológiai jellegű károk (rendkívüli erejű vihar, villámcsapás);

b.) Civilizációs, ipari katasztrófák
- nukleáris balesetek (erőművi balesetek);
- veszélyes anyagok kikerülése (gyárak, üzemek, raktárak szállítójárművek sérülése, robbanások);
- közlekedési balesetek (közúti, vasúti jármű, repülőgép véletlen vagy szándékos becsapódása);

c.) Terrorizmus
- robbantások, támadások (állami intézmények, távvezetékek, hírközpontok, adók, légiforgalmi létesítmények, internet szolgáltatók, stb. ellen);
- a fenti rendszereket üzemeltető kulcsfontosságú személyek kiiktatása;
- bűnözés (adatok erőszakkal való megsemmisítése, megszerzése, irányítórendszerek befolyásolása, megbénítása);

d.) Fegyveres konfliktusok
- háborúk;
- fegyveres csoportok támadása;
- belső fegyveres konfliktusok, polgárháborúk, sztrájk.

Egyenként vizsgálva a különböző veszély típusokat könnyen belátható, hogy a természeti katasztrófák elleni felkészülés többnyire gondos tervezéssel biztosítható, és ezáltal a kár bekövetkezése jó eséllyel a lehetőségekhez képest a legkisebbre csökkenthető. A mégis bekövetkező eseményeknél a kárelhárítás – elsősorban itt is a jó tervezhetőség miatt – gyorsan és hatékonyan véghezvihető. Hasonló a helyzet a civilizációs jellegű katasztrófák esetében is. Igaz itt már előfordulhatnak előre nem tervezhető mértékű, nagy területi kiterjedésű katasztrófa sújtotta területek, városok és régiók, amelyeken belül lehetnek kritikus információs infrastruktúrák.

A terrorizmus elleni védelem napjaink kiemelt fontosságú területe. Bár Magyarország eddig nem tartozott a terrorszervezetek elsődleges célországai közé, nem szabad elfelejtenünk, hogy hazánk elkötelezett szövetségese a NATO-nak, amelynek keretében több konfliktus övezetben katonai erővel jelen van és várhatóan a jövőben is lesz katonai szerepvállalásunk. Mindezeken túl teljes jogú tagjai vagyunk az Európai Uniónak. Szövetségeseink között tehát ott vannak a terrorszervezetek elsődleges célországai, illetve ezen célországoknak különféle politikai, gazdasági képviseletei, érdekeltségei hazánk területén is megtalálhatók. Ezért a védelmi felkészülés szempontjából komolyan kell venni a terror veszélyeztetettségből adódó védekezést. A terrorizmussal kapcsolatos veszélyek felsorolásánál csak a fantázia szabhat határt, ezért a létesítmények védelmének kialakításánál e területet jól ismerő, terrorelhárításban jártas szakemberek bevonása szükséges.

2.1.2. FENYEGETÉSEK AZ INFORMÁCIÓS DIMENZIÓBÓL

A kritikus infrastruktúrákra leselkedő infokommunikációs fenyegetettségeket a támadó, valamint az elkövetés módja alapján csoportosíthatjuk. Az elkövető szándéka és rendelkezésére álló erőforrásai szintén eltérőek lehetnek.

A kritikus információs infrastruktúrákat veszélyeztető tényezők lehetnek:

- a tévedő alkalmazottak;
- az elégedetlen alkalmazottak vagy szerződéses partnerek;
- a hackerek[33];

[33] A hacker az informatikai rendszerbe informatikai eszközöket használva, kifejezett ártó szándék nélküli betörő. Célja kizárólag a programok védelmének feltörése, kijátszása. Eredeti jelentése szerint a hacker olyan mesterember, aki fából tárgyakat farag. A tömegkommunikációban helytelenül minden számítógépes betörőre használják. A cracker az, aki az informatikai rendszerbe informatikai eszközöket használva, direkt rombolási céllal tör be. A crack eredeti jelentése: valami keménynek (pl. dióhéjnak) az összeroppantása, feltörése. [85]

– a személyes előnyöket keresők, pl.: zsarolás, lopás;
– a szervezett bűnözés ügynökei, kereskedelmi versenytársak vagy más érdekcsoportok;
– külföldi kémszervezetek;
– terroristák;
– ellenséges fegyveres erők.

A fenti csoportok forrásai és szakértelme eltérő lehet. *„A fenyegetések származhatnak egyes személyektől, jogosulatlan felhasználóktól, terroristáktól, különböző nemzeti szervezetektől, külföldi hírszerző szolgálatoktól vagy akár katonai szervezetektől is. Az infokommunikációs rendszer elleni tevékenység eredetét nehéz azonosítani, mivel e csoportok között a határok elmosódnak …”* [45]

Az infokommunikációs[34] eredetű támadások közé tartozik többek közt:

– szolgáltatás megtagadás jellegű támadás[35];
– cracking vagy hacking[36], ha rendszerkárokhoz vagy a bizalmasság sérüléséhez vezet;
– fedett vagy rosszindulatú (malware) programok, beleértve a vírusokat[37], férgeket[38], trójai programokat[39], hoaxokat[40];

[34] A katonai vezetési rendszerek, kommunikációs rendszerek, fegyverirányító rendszerek és a katonai célokra felhasználható polgári rendszerek elemeinek fizikai megsemmisítése, pusztítása [42] ugyan az infokommunikációs rendszer ellen irányul, de ez a fizikai fenyegetések körébe tartozik.

[35] Distributed Denial of Service (DDoS). Olyan logikai támadás, amely az informatikai rendszer egy (vagy több) kiszolgálóját tömeges szolgáltatás igénnyel túlterheli, ami a felhasználók hozzáférését nehezíti, vagy akár a kiszolgáló teljes leállásához is vezethet. [85]

[36] A hacking és a cracing az informatikai rendszerbe informatikai eszközöket használó betörés. A hacking kifejezett ártó szándék nélküli, szemben az elsődlegesen károkozásra, esetleg nyereségre irányuló cracking-gel. [85]

[37] Olyan programtörzs, amely a megfertőzött program alkalmazása során másolja, esetleg kis mértékben változtatja (mutálja) önmagát. Valamilyen beépített feltétel bekövetkezésekor többnyire romboló, néha csak figyelmeztető vagy „tréfás” hatású kódja is elindul. Többnyire komoly károkat okoznak, adatot törölnek, formázzák a merevlemezt, vagy az adatállományokat küldik szét e-mail-ben. [85]

[38] Worm. Olyan program, amely a számítógép hálózaton keresztül, a hálózati funkciók kihasználásával terjed számítógéptől számítógépig és károkozó hatását önmaga – a számítógép összeomlásáig tartó – reprodukálásával, továbbításával éri el. [85]

[39] Trojan horse. Más néven *trójai faló*, olyan kártékony program, amelyet alkalmazásnak, játéknak, szolgáltatásnak, vagy más egyéb tevékenység mögé rejtenek, álcáznak. Futtatásakor fejti ki károkozó hatását. [85]

[40] Olyan e-mail, ami valamilyen új – általában fiktív – vírus terjedésére figyelmeztet, és a fertőzés megakadályozása érdekében egy vagy több fájl törlésére ösztönöz (ezek azonban a rendszer működéséhez szükséges, de kevésbé ismert állományok). Az e-mail továbbküldésére is buzdít, hogy a levéláradat – lánc-levél – szűk keresztmetszetet generáljon a hálózaton. [85]

- adathalászat (phishing) bizalmas adatok megszerzésére;
- a programok hibáinak kihasználásával elkövetett betörés (botnets);
- üzenetek jogtalan elfogása vagy lehallgatása (pl.: laptop vagy PC-k lopása, forgalom eltérítések, billentyűzet vagy hálózat lehallgatása, stb.);
- belső munkatársak szándékos vagy gondatlan károkozása;
- elektronikai felderítés útján az infokommunikációs rendszer adatainak megszerzése;
- irányított energiájú fegyverekkel[41] elkövetett támadások;
- egyéb elektronikai támadások[42].

Amióta az internet mindenütt jelenlévővé vált az információs társadalomban, a legtöbb támadás megvalósítása is áttevődött az internetre. Az internet alapú támadások sajátos jellegei önmaguk megmagyarázzák azok gyakoriságát és hatását:

1. Az internet lehetővé teszi a nagy távolságokról történő támadásokat, amelyek magasabb fokú anonimitást és védelmet biztosítanak az elkövető számára. Ez a sajátosság csökkenti a jogszabályok hatékonyságát is. Számos esetben a támadásokat a nemzeti határokon túlról intézik.
2. Az internetes támadások során is gyakran használják fel a számítógépeket bizonyos eljárások automatikus ismétlődésére, mint például a szótár alapú kereső programok jelszavak feltörésére, vagy vírusok, melyek korlátlanul sokszorozzák önmagukat. Ez a sajátosság kiegészítheti az egyén szakértelmét globális kihatással járó infrastruktúra támadásra is. Ilyen esetben a bekövetkezett hatás nincs összefüggésben a támadó rendelkezésére álló erőforrásokkal.
3. Előre megírt, automatizált támadási eszközök egyre szélesebb körben elérhetőek az interneten, és olyan személyek által is használhatóvá válnak, akik nincsenek tisztában magával az eszközzel vagy a hatásukkal, illetve önmaguk képtelenek is lennének ilyeneket előállítani.

Az internet számos más lehetőséget biztosít a reá kapcsolódott rendszerek megtámadására. A következőkben egy valóságos eseményt szeretnék bemutatni a kritikus információs infrastruktúra támadhatóságát bizonyítandó.

[41] Irányított energiájú fegyverek közé tartoznak pl. az elektromágneses impulzus (EMP) fegyverek.

[42] Egyéb elektronikai támadás pl. az elektronikai zavarás.

Egy esettanulmány – az észt-orosz kiberháború

2007 májusában Észtország internetes hálózata szinte teljesen megbénult. *Tallin felszabadítóinak szovjet emlékműve* áthelyezése miatt rendszeres internetes támadásokat szerveztek főként Észtországon kívülről az észt államigazgatás hivatalos kommunikációs vonalainak és weboldalainak blokkolására irányuló kísérletek keretében. Emellett az interneten és mobiltelefon-üzeneteken keresztül folytatódtak az intenzív propaganda-támadások, amelyek fegyveres ellenállásra és további erőszakra szólítottak fel.

Az okokat minden elemző szerint külső terhelések kényszerítették ki. Az első forgalombénító DDoS-támadások május elején kezdődtek, célpontjaik a parlament, a kormányhivatalok, sőt a bankok és az észt média számítógépes központjai voltak. Az észt hálózaton az adatforgalom sokszor órákon át a normális ezerszerese volt. Az ország internetes forgalmát irányító központok napjában többször leálltak, az állami szervek hálózatait le kellett választani az internetről. A banki rendszerek megbénultak, a pénzügyi megbízások rendszeresen akadoztak. A támadások azért is érintették érzékenyen a balti államot, mert kiugróan fejlett az ország internetes kultúrája.

Május közepén tetőzött a támadási hullám, de ezt követően – ugyan kisebb intenzitással – azonban továbbra is folyt a túlterheléses támadás. Számos hálózati rendszer még hetekig csökkentett üzemmódban volt csak képes dolgozni. Május 15-én például az ország második bankja, a SEB Eesti Uhisbank a tömeges internetes támadások miatt kénytelen volt felfüggeszteni azt a szolgáltatását, hogy külföldről is be lehet lépni a pénzintézet egyes rendszereibe. Egy észt bank, a Hansabank nyilvánosságra hozta a támadások miatti veszteségét. A jelentés szerint május 10-én több mint egymillió dolláros forgalomkiesést szenvedtek el.

Az elemzők szerint az akciók túlságosan jók és összehangoltak voltak ahhoz, hogy mindössze néhány rosszindulatú programozót feltételezzenek csak a háttérben. Néhány támadást sikerült orosz szerverekig visszanyomozni, sőt az Európai Parlament állásfoglalásában leszögezte, hogy e támadások az orosz közigazgatás IP címeiről érkeztek, de az alkalmazott technika miatt rendkívül nehéz a forrásokat pontosan meghatározni.

Az Európai Parlament 2007. május 24-én állásfoglalást adott ki az ügyben. A NATO május közepén szakértőt küldött Észtországba, hogy kivizsgálja a történteket, és segítsen kivédeni a további támadásokat.

Az online beavatkozást sem az észtek, sem az EU, sem a NATO nem minősítette katonai akciónak! A NATO nyilvánosan nem foglalt állást abban a kérdésben, hogy kik

voltak a támadók, kinek az irányításával történt, támadásnak minősíti-e az eseményeket. A NATO illetékese elmondta, hogy a katonai szövetség megvizsgálta, milyen hatásai lehetnek ezeknek az akcióknak, és folyamatos kapcsolatban állt az észt szervekkel. A NATO észtországi rendszereit mindenesetre nem érte internetes támadás – tette hozzá.[14], [18], [20]

A fentiek jól jellemzik, hogy egy internetes támadás milyen károkat képes okozni, ugyanakkor még a támadó személyének a megállapítása is gondot okoz. Bár kezdetben az észt miniszterelnök kijelentette, hogy *Észtországban kiberháború folyik* [14], sőt *a NATO egyik tagja elleni támadás az egész katonai szövetség elleni támadásnak minősül* nyilatkozott egy NATO-tisztségviselő [20], később a konfliktus teljes feltárása, a valós támadó felelősségre vonása lekerült a (nyilvános) napirendről.

A fentiek is alátámasztják azt a véleményemet, hogy az információs dimenzióból érkező támadások, a támadás előkészületei csak nagyon alacsony hatékonysággal deríthetők fel. Kisszámú elkövető készül fel a támadásra, ez megkönnyíti a konspirációt. Nincsenek látható csapatmozgások, nincs szükség utánpótlási vonalak kiépítésére, nem kell hadianyagokat előkészíteni, ami a vizuális felderítést kapcsolja ki. Az illegális fegyverkereskedelem, és más szokványos csatornák figyelése sem hoz értékelhető információt ebben az esetben. A titkosszolgálati módszerekkel megszerezhető információ mennyisége is rendkívül kevés, ezek is nehezen ellenőrizhetőek, így elemzésük nem vezethet eredményre. Az előkészületek felismerhetőségének hiánya miatt nincs *veszélyeztetettségi időszak*, a támadás váratlanul érkezik. Ezért fontos ezen a területen a békeidőszakban is hatékony felkészülés és a folyamatos monitorozás, hogy az esetleges támadást már korai szakaszában észleljük.

A támadás blokkolására, illetve bármilyen ellentámadásra ma még nincs hatékony infokommunikációs eszköz a kezünkben. Ugyanakkor – éppen e tényből következően – elengedhetetlenül fontos a megelőzés, a jogszabályoknak, szabványoknak, ajánlásoknak megfelelően felépített, megfelelő tartalékolással rendelkező biztonságos rendszerek kialakítása.

2.2. A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELME NEMZETKÖZI TÉREN

2.2.1. A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELMÉRE VONATKOZÓ RELEVÁNS NEMZETKÖZI ELŐÍRÁSOK ÉS AJÁNLÁSOK

A hazai védelmi előírásoknak összhangban kell lenniük a NATO és az Európai Unió előírásaival és elvárásaival. Figyelembe kell venni a nemzetközi szabványokat, a mérvadó ajánlásokat, így koherens szabályozásokban rendelkezni kell az állami irányítás és felügyelet megoldásáról, az infokommunikációs rendszerek, eszközök biztonsági elvárásairól, követelményeiről és a vizsgálatuk szabályairól. Ezért elengedhetetlen a nemzetközi, külföldi és a hazai jogszabályok, szabványok, ajánlások ismerete, a hazaiak felhasználási helyzetének elemzése.

Zöld könyv a kritikus infrastruktúrák védelmére vonatkozó európai programról

Az Európai Unió a cselekvés szükségességét felismerve számos ország tapasztalatainak elemzését követően nemzetközi szinten a kritikus infrastruktúrák védelmével kapcsolatos uniós szintű koncepcióját, illetve szabályozási elgondolását a *Zöld könyv a kritikus infrastruktúrák védelmére vonatkozó európai programról* [100] anyagban, továbbá *Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló tanácsi irányelvben* [28] fejti ki. A kritikus európai infrastruktúrák védelmének javítása érdekében egy sor új intézkedést javasol. E kezdeményezés célja annak biztosítása, hogy a kritikus infrastruktúrák megzavarása vagy manipulálása a lehetséges mértékben rövid, kivételes, kezelhető és földrajzilag behatárolt legyen, valamint hogy minimalizálja annak végzetes következményeit. [29]

Meghatározásra kerül a kritikus infrastruktúra definíciója, és elemei *alágazatokra* lebontva. Mind a Zöld Könyv, mind a tanácsi irányelv részletes segítség az európai kritikus infrastruktúrák azonosításához, a kritikus infrastruktúrák védelmének értelmezéséhez.

Az elektronikus kommunikációs infrastruktúra elérhetősége és robosztussága

Az Információs Társadalom és Média Főigazgatóság[43] (a továbbiakban: DG INFSO) megrendelt egy *Az elektronikus kommunikációs infrastruktúra elérhetősége és*

[43] Directorate-General for Information Society and Media (DG INFSO)

robosztussága[44] című tanulmányt [16] (a továbbiakban ARECI), melynek főbb megállapításai 10 ajánlásban foglalhatók össze, ebből öt a hálózati elérhetőséggel, öt pedig a robosztussággal kapcsolatos. Az ajánlások kapcsán hangsúlyozni kell, hogy azok – még – nem az EU Bizottság hivatalos álláspontját képviselik, ugyanakkor, amennyiben a Bizottság elfogadja a tanulmányt, úgy mindenképpen a hivatalos ajánlások alapját jelenthetik.

Az ajánlásban kidolgozott legjobb gyakorlatot[45] bemutató eljárások csak ajánlások, és ezek egyelőre jogszabályi szinten kötelező rendelkezésekként nem jelennek meg az európai intézmények tervei között. Az ajánlások az alábbi területekre terjednek ki:

1. energiaellátás;
2. hardver;
3. szoftver;
4. hálózat;
5. hálózati forgalom;
6. stratégia.

Kritikus Infrastruktúrák Védelme – Koncepció

A NATO EAPCP (SCEPC) *Critical Infrastructure Protection – Concept Paper* dokumentuma a kritikus információs infrastruktúrák területén történő együttműködésről szól. A koncepció vázlatos rövid, közép és hosszú távú terveket tartalmaz az együttműködés formáiról. A rövid távú terv a kritikus infrastruktúrák tudatosításáról, oktatás és képzés bevezetéséről, információ megosztásról, a kritikus infrastruktúrák meghatározásáról és gyakorlásról szól. A kritikus információs infrastruktúra kérdései nem jelennek meg a koncepcióban. [39]

A NATO Polgári Vészhelyzeti Tervezés (NATO Civil Emergency Planning – CEP) 2005-2006 számára kiadott miniszteri irányelvek számos utalást adnak a kritikus infrastruktúrák védelmére. [56]

Mint a fentiekből is látható a kritikus infrastruktúrákkal, és különösen a kritikus információs infrastruktúrákkal kapcsolatos szabványok és ajánlások még váratnak magukra. A kritikus információs infrastruktúrák védelméhez szorosan kapcsolódó infokommunikációs biztonsági szabványokat és ajánlásokat bemutatom.

---

[44] Availability and Robustness of Electronic Communications Infrastructures, "The ARECI Study"

[45] ang.: best practice

Infokommunikációs szabványok és ajánlások

Common Criteria

A TCSEC és az ITSEC problémáinak feloldására az Egyesült Államokban és Kanadában elkészültek az FC[46], illetve a CTCPEC[47] dokumentumok. Az FC dokumentumnak az 1993-ban az Európai Közösség illetékes bizottságának történt bemutatása után az a határozat született, hogy az ITSEC, a CTCPEC és az FC szerzői dolgozzanak ki egy olyan követelményrendszert, amely nemzetközileg elfogadható lesz, és az ISO/IEC számára ajánlani lehet a szabványosítási munka alapjául. Ezzel egy időben a Nemzetközi Szabványosítási Szervezetben (ISO[48]) és a Nemzetközi Elektrotechnikai Bizottságban (IEC[49]) is elkezdődött ebben a tárgyban a munka, ez azonban a nemzeti szinteken addig kidolgozott követelmények egyeztetése miatt viszonylag lassan haladt előre.[85]

Az Európai Közösség, valamint az amerikai és a kanadai kormányok támogatásával kidolgozásra került Common Criteria (CC)[50] dokumentum, azaz az ISO/IEC 15408 (*Common Criteria for Information Technology Security Evaluation*, *version 2.0*) szabvány elsősorban technikai jellegű, főleg az informatikai termékek gyártóinak ad támogatást. Nagyon részletes és megbízható követelményeket, eljárásokat biztosít az informatikai eszközök biztonsági minősítésére. Nem tartalmaz ugyanakkor követelményeket az informatikai rendszerek üzemeltetésével, működtetésével kapcsolatban a felhasználó szervezetek számára. [58], [59], [60]

A Magyar Szabványügyi Testület 2002-ben magyar szabványként kiadta *Az informatikai biztonságértékelés közös szempontjai* címen az ISO/IEC 15408 szabványt.

A CC feldolgozására és honosítására irányuló munka hazánkban 1997-ben kezdődött, majd 1998-ban a MeH ITB 16. sz. ajánlásaként *Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertana* címen, mint a Common Criteria 1.0 változatának hazai feldolgozása kiadásra került.

---

[46] FC: Federal Criteria for Information Technology Security (Az Információtechnológia Biztonságára vonatkozó Szövetségi Kritériumok)

[47] CTCPEC: Canadian Trusted Computer Product Evaluation Criteria (A Biztonságos Számítástechnikai Termékek Értékelési Kritériumai Kanadában)

[48] ISO: International Organization for Standardization

[49] IEC: International Electrotechnical Commission)

[50] CC: Common Criteria (Közös Követelmények)

ISO/IEC 27000 (BS 7799, ISO/IEC 17799)

2005. október 14-én a Nemzetközi Szabványügyi Testület kiadta az ISO/IEC 27001:2005 szabványt, *Informatika – Biztonsági technikák – Informatikai biztonság irányítási rendszerek – Követelmények*[51] címmel. A szabvány a BS 7799-2:2002 brit szabvány nemzetközi megfelelője. [65]

Az új szabvány megjelenése az informatikai biztonság irányítási rendszerének fejlesztésére és nemzetközi szabványként történő népszerűsítésére fordított munka eredménye.

Az új számozás nem következik a régiekből, hanem egy új biztonsági szabványcsalád, az ISO 27000 megteremtésének tervéből fakad. Az ilyen tevékenység célja valamennyi, az infokommunikációs biztonság irányításával (menedzselésével) foglalkozó szabvány egyetlen sorozatba gyűjtése. A szabványcsalád jelenleg tervezett tagjai:

- **ISO/IEC 27000** – Szószedet és terminológia (definíciók a sorozat összes szabványához). Jelenleg ez a szabvány fejlesztés alatt áll.
- **ISO/IEC 27001** – Az informatikai biztonság irányítási rendszere (BS 7799-2:2002), a szervezet auditálásához szükséges (megfelelőségi) előírások. Az ISO/IEC 27001 szabványt 2005. 10. 14 –én tették közzé ISO/IEC 27001:2005 számon.
- **ISO/IEC 27002** – Az ISO/IEC 17799:2005 szabvány utódja, azzal gyakorlatilag megegyezik. Az informatikai biztonság irányítása gyakorlati előírásait, ellenőrzési célokat és a legjobb gyakorlatot (best practice) írja le.
- **ISO/IEC 27003** – Az ISO/IEC 27000 szabvány implementálásához szükséges tanácsokat és útmutatókat fogja tartalmazni. Jelenleg ez a szabvány még csak terv formájában létezik.
- **ISO/IEC 27004** – Egy új szabvány lesz, amely az informatikai biztonság mérésével fog foglalkozni, abból a célból, hogy az informatikai biztonság irányítási rendszerének hatékonyságát mérni tudjuk. Jelenleg előkészületben van az ISO/IEC 27004 szabvány, amely az *Informatika – Informatikai biztonság irányítási mérések*[52] előzetes címet viseli. Jelenleg ez a szabvány még csak terv formájában létezik.

[51] Information Technology – Security techniques – Code of Practice for Information Security Management

52 Information technology – Security techniques – Information Security Management Measurements

- **ISO/IEC 27005** – Az informatikai biztonság kockázatkezelésével foglalkozik. Az ISO/IEC 13335-3:1998 és az ISO/IEC 13335-4 :2000 szabványok felülvizsgálatával készül. Jelenleg ez a szabvány fejlesztés alatt áll.
- **ISO/IEC 27006** – az ISO/IEC IEC 27001 szabványnak való megfelelést vizsgáló szervezetek számára tartalmaz követelményeket. 2007. február 13-án tették közzé.
- **ISO/IEC 27011** – informatikai biztonságirányítási irányelvek a telekommunikációnak. Jelenleg ez a szabvány fejlesztés alatt áll.

Az ISO/IEC 27001:2005 (BS 7799-2)

A BS 7799 2. részének fejlesztése során került előtérbe a szervezeti szintű informatikai biztonságirányítási rendszer (ISMS[53]), amely alapvetően meghatározza a 2. rész szellemét. Ettől a 2. rész még az első résznél is nagyobb jelentőségű lett, mert meghatározza a megfelelőségi és ellenőrzési követelményeket, azaz a szervezetek vezetése számára meghatározza azokat a teendőket, amelyekkel az informatikai biztonsági rendszert irányíthatja, csökkentheti a maradék kockázatokat, valamint ellenőrizheti a jogszabályoknak, a tulajdonosok és az ügyfelek által támasztott biztonsági követelményeknek való megfelelést. [85]

A BS 7799 második részét 2002-ben módosították az ISO 9001:2000 és az ISO 14001:1996 szabványokkal való harmonizáció miatt. Az aktuális változat a *BS 7799 Part 2:2002, Information security management systems – Specification with guidance for use.* Ez utóbbit fogadta el a Nemzetközi Szabványügyi Testület **ISO/IEC 27001:2005** (*Informatika – Biztonsági technikák – Informatikai biztonság irányítási rendszere – Követelmények*.) számon nemzetközi szabványként. [65]

ISO/IEC 27002:2005 (ISO/IEC 17799:2005, BS 7799-1)

Egyes országokban megindult olyan ajánlások, követelmények fejlesztése is, amelyek kifejezetten a felhasználók számára nyújtanak segítséget egy, a teljes szervezetet és minden rendszerelemet átfogó informatikai biztonságmenedzsment rendszer megvalósítására és ellenőrzésére. A Brit Szabványügyi Hivatal[54] *BS 7799 Part 1, Code of practice for information security management* című kiadványát 2000 augusztusában ISO/IEC 17799:2000 számon *Information Technology – Code of practice for information security management*

[53] ISMS: Information Security Management System

54 British Standard Institute

néven nemzetközi szabványként fogadták el. [61] Az eddig többségében termékorientált szemlélet egy szervezeti szintű informatikai biztonságmenedzsment központú szemlélet váltotta fel. Az ISO/IEC 17799 szabvány alapvetően abban különbözik a korábbi informatikai biztonsági ajánlásoktól, hogy nem követelményeket ír elő, hanem – a minőségbiztosításról szóló ISO 9000 szabványhoz hasonlóan – *a teljes körű informatikai biztonság* megteremtéséhez szükséges szervezési, szabályozási szempontrendszert adja meg. A szabvány felhasználóinak a biztonsági követelményeket, intézkedéseket a szervezet üzleti céljaiból és stratégiájából kell levezetniük. Ez a szabvány már alkalmas arra, hogy a megfelelő akkreditálás és tanúsítási eljárások alkalmazásával lehetővé váljon a teljes informatikai rendszer értékelése és tanúsítása. [85]

Ellentmondásosnak tűnhet, hogy az ISO/IEC 17799 csak a figyelembe veendő biztonsági követelményeket és a megvalósítandó védelmi intézkedéseket írja le, de nem foglalkozik a megfelelőségi és ellenőrzési követelményekkel. Ezt az ISO/IEC 27001:2005 (BS 7799 2. rész) tartalmazza.

Az ISO/IEC 17799 szabvány nem csak azért kiemelt fontosságú, mert a teljes szervezetre vonatkozó, az összes rendszerelem csoportot átölelő informatikai biztonsági követelményeket és védelmi intézkedéseket tartalmazza, de a különböző nemzeti dokumentumok közül ez vált nemzetközi szabvánnyá, és emellett a nemzetközi szabvánnyá vált ITIL is ezt használja hivatkozási alapként.

Az ISO/IEC 17799 szabványt – bár kritikák is érik – a világ, és különösen az Európai Unió mind több országában fogadják el a különböző szervezetek informatikai rendszerük biztonságának alapjaként.

2005. június 10-én kiadták ISO/IEC 17799:2005 számon az informatikai biztonság e szabványának új verzióját [62], amit 2007 júliusában kis javításokkal már a 27000-es sorozat részeként ISO/IEC27002:2005 számon publikáltak.

A szabvány új címe: *Informatika – Biztonsági technikák – Kézikönyv az informatikai biztonság irányításához*[55]. A szabvány fő fejezetei megegyeznek a 2000. évi kiadásban szereplőkkel, de kiegészült egy új informatikai biztonsági eseménykezelési (incidensmenedzsment) fejezettel. Változott viszont az egyes pontokhoz írt útmutatók struktúrája, új elemek is belekerültek (pl. olyanok is, melyek a BS 7799-2:2002 fő részében szerepelnek). [66]

55 Information technology – Code of practice for information security management

A Magyar Szabványügyi Testület 2002. évben magyar szabványként kiadta *Az informatikai biztonság menedzsmentjének eljárásrendje* címen az ISO/IEC 17799:2000 szabványt. Sajnos az MSZ ISO/IEC 177999:2002 magyar szabványnak van egy nagy hibája. Nem az informatikai és a biztonsági szaknyelvezetet ismerő fordító kezéből került ki, ezért számos, a szakmában értelmezhetetlen kifejezést tartalmaz (pl.: user=használó, vagy terminal time-out=végállomás időlekapcsolás), ami miatt a magyar felhasználók nem szívesen használják.

ISO/IEC TR 13335

Az informatikai biztonság területén egyre többen használják az *ISO/IEC TR 13335 – Guidelines for the Management of IT Security*[56] (GMITS) műszaki jelentést. Az ISO/IEC TR 13335 nem szabvány, annak ellenére, hogy a Nemzetközi Szabványosítási Szervezet és a Nemzetközi Elektrotechnikai Bizottság szabványsorozatának részeként került kiadásra, de *Technical Report*-ként. Ebben az esetben ez a megoldási lehetőségek leírását jelenti, és ezt csak akkor vizsgálják felül, ha az abban foglaltak már nem érvényesek, vagy már nincsenek használatban.

Az ISO/IEC TR 13335 öt részből áll:

1. Az informatikai biztonság koncepciója és modellje (Concepts and models for IT Security) [57];
2. Az informatikai biztonság irányítása és tervezése (Managing and planning IT Security) [72];
3. Az informatikai biztonság irányításának megoldásai (Techniques for the Management of IT Security) [73];
4. A védelmi eljárások kiválasztása (Selection of Safeguards) [74];
5. Hálózatbiztonsági megoldások (Safeguards for External Connections) [75].

A Magyar Szabványügyi Testületnél jelenleg előkészítés alatt áll az ISO/IEC TR 13335 első és második részének magyar kiadása.

[56] Segédlet az informatikai biztonság irányításához

Az informatikaszolgáltatás módszertana

Az informatikai biztonság kérdésével számos szabvány és ajánlás foglakozik. Gyakran hivatkoznak ezen a területen az ITIL[57]-re és a COBIT[58]-ra.

Az ITIL kezdetben brit szabvány (BS 15000) és kormányzati ajánlás volt, és a közigazgatási területen általában megkövetelték az alkalmazását. Mivel a gyakorlati alkalmazás tapasztalatai kedvezőek voltak, a módszertant a piaci környezetben is egyre inkább használni kezdték. Az ITIL egyre inkább elterjedt a szigetországon kívül is. Egyre több országban alakultak helyi *Fórumok*, amelyek összefogására létrejött az *IT Service Management Forum International*. Ez a nemzeti fórumokon keresztül egyrészt segítette az ITIL terjedését, másrészt ügyelt arra, hogy az egységes maradjon. Az ITIL mára gyakorlatilag nemzetközi szabvánnyá vált, amelynek több országban működik felhasználói szervezete, meghatározó módszertanná vált az informatikai infrastruktúra és informatikaszolgáltatás irányítása területén. Az ITIL-t számos nemzetközi informatikai cég is elfogadta és támogatja, így például a Hewlett Packard, Microsoft, IBM stb. Ezek a cégek saját gyakorlatukba beépítették az ITIL terminológiáját és megközelítését. Sok szolgáltató, amely támogató szoftver eszközöket kínál, igyekszik azokat ITIL konformmá tenni, hogy ezzel is javítsa piaci pozícióját.

Az ITIL-t a MeH ITB Infrastruktúra menedzsment címen 15. számú ajánlásaként kiadta, majd az ITIL 3.1 verzióját a Széchenyi-terv támogatásával 2002 novemberében honosították.

Összefoglalva, az ITIL, azaz *informatikaszolgáltatás módszertana* az informatikára, mint szolgáltatás egészére kiterjedő, nemzetközileg széles körben elfogadott dokumentum. Az ITIL Biztonságirányítás (Security Management) kötete a BS7799 szabványt használja hivatkozásként, valamint a létező ITIL folyamatokat bővíti a biztonságirányítással. [85], [63], [64]

COBIT

Az Informatikai Irányítási és Ellenőrzési Módszertan[59] támogatói, az Information Systems Audit and Control Foundation (Információs Rendszerek Ellenőrzésével és Vizsgálatával foglalkozó Alapítvány) és az IT Governance Institute elsősorban azzal a céllal dolgozták ki az

[57] ITIL: IT Infrastructure Library, Az informatikaszolgáltatás módszertana

[58] COBIT: Control Objectives for Information and Related Technology (Information Systems Audit and Control Foundation és IT Governance Institute)

[59] Control Objectives for Information and Related Technology

Összefoglaló áttekintés, a *Keretrendszer,* az *Ellenőrzési irányelvek,* a *Vezetői útmutató,* az *Auditálási útmutató* és az *Alkalmazási módszerek* elnevezésű kiadványokat, hogy forrásanyagot biztosítnak az ellenőrzési szakemberek számára. A COBIT az üzleti folyamatokra, valamint az ezeket támogató informatikai megoldások négy területére – tervezés és szervezés; beszerzés és üzembe állítás; informatikai szolgáltatás és támogatás, valamint felügyelet – helyezi a fő hangsúlyt. A COBIT az informatikai rendszerek szervezéséhez, és különösen az ellenőrzéséhez szükséges irányelveket tartalmazó dokumentum, amely a biztonság kérdésére nagy hangsúlyt fektet, de annak részleteivel nem foglalkozik.

Az ISACA és az IT Governance Institute 2004-ben a *Mapping of ISO/IEC 17799:2000 with COBIT* (2004) kiadványban már az ISO/IEC 17799 szabvánnyal hangolja össze a COBIT Framework-ben leírt informatikairányítási keretrendszert.

A COBIT 4. biztonsági szempontból is jelentős előrelépés. Többek között megjelent a legjobb informatikai biztonsági gyakorlatra, az ISO/IEC 17999 szabványra, az ITIL-re, és az ISF Good Practice for Information Security ajánlásra való hivatkozás. Bár a fizikai biztonság már önálló ellenőrzési célként szerepel, de még korántsem teljes körűek a fizikai biztonsági célok.[31]

2.2.2. A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELMÉNEK NEMZETKÖZI GYAKORLATA

A kritikus információs infrastruktúrák védelmének hazai lehetőségei elsősorban a szövetséges országok gyakorlata alapján analizálható. Az egyes országok méretük, fenyegetettség-érzetük és nem utolsó sorban gazdasági potenciáljuk szerint reagáltak a kritikus információs infrastruktúrák védelmének kérdéseire. Az Amerikai Egyesült Államok – a 2001. szeptember 11-i terrortámadás egyik reakciójaként – 2002-ben létrehozta a Belbiztonsági Minisztériumot, a Department of Homeland Security-t, amely az egyik kulcsintézménye a nemzeti kritikus infrastruktúrák védelmi stratégiájának. Az Egyesült Királyságban a létfontosságú nemzeti infrastruktúrák információs biztonságának megteremtésére egy tárcaközi központot hoztak létre. Németországban a Szövetségi Belügyminisztériumban is működik egy munkacsoport a kritikus infrastruktúrák védelmére.

2.2.2.1. Az Európai Unió

Európában az információs társadalom megjelenése vezetett annak a felismerésére, hogy olyan környezetet kell létrehozni, melyben megbízható, biztonságos információs infrastruktúrákat lehet kialakítani. Európa egyre erősödő függése az elektronikus kommunikációtól és információáramlástól a létfontosságú üzleti és társadalmi folyamatokat sérülékenyebbé tették az információs hálózatok véletlenszerű vagy szándékos hibáival szemben.

Az alábbiakban két kezdeményezést kívánok bemutatni, amelyek európai uniós szintre próbálták, illetve próbálják emelni a leginkább a tagállamok nemzeti biztonsági kérdéskörébe tartozó terület egyes vonatkozásait, és amelyek ennek következtében leginkább tagállami ellenállásba ütköznek.

Kritikus Infrastruktúrák Védelmi Európai Program

Az EU kritikus infrastruktúrák védelemre vonatkozó stratégiai koncepciójának kidolgozása 2004 júniusában kezdődött meg. A terrorizmus elleni harc deklarálását követően az Európai Bizottság felkérte a közös kül- és biztonságpolitika képviselőit, hogy készítsék elő a kritikus infrastruktúrák védelmének átfogó stratégiáját. [50]

A kritikus infrastruktúrák védelmére vonatkozó európai programjavaslat szerint a kritikus infrastruktúrák nagy száma és sajátosságaik miatt lehetetlen mindegyik védelmét európai szintű intézkedéssel biztosítani. A szubszidiaritás elvének alkalmazásával uniós szinten a nemzeti határokon átterjedő hatással rendelkező kritikus infrastruktúrákra kell koncentrálni, a többi védelmét meghagyva – bár közös keretmegoldások között – a tagállamok önálló felelősségében.

Az *Európai Kritikus Infrastruktúra Védelmi Program*[60] (a továbbiakban: EPCIP) célja az Unió kritikus infrastruktúrái folyamatos működtetésének biztosítása, a biztonság megfelelő és egységes szintjének garantálása, az iparágak és tagállamok kormányainak támogatása az EU valamennyi szintjén.

Az EPCIP célkitűzéseit a következőkben határozták meg:

- a kritikus infrastruktúrák meghatározásának folytatása;
- sérülékenységek és függőségek elemzése;
- megoldások indítványozása valamennyi veszéllyel kapcsolatos védelem és felkészülés tekintetében;
- kockázatfelmérések készítése.

[60] European Programme for Critical Infrastructure Protection (EPCIP)

A program végrehajtásához a kritikus infrastruktúrák tulajdonosainak és működtetőinek, a szabályozók, szakmai szervezetek és ágazati szövetségek, valamint a tagállamok és a Bizottság aktív részvétele szükséges. A javaslat szerint az EPCIP működésében szerepet kell játszania a Rendőrségi Vezetők Munkacsoportjának, illetve az Europolnak is, elsősorban az információterjesztés területén. A tagállamok feladata a nemzeti szempontból kritikus infrastruktúrák adatbázisainak kialakítása/megtartása és fenntartása, a vonatkozó tervek kialakítása, jóváhagyása és ellenőrzése a hatáskörükbe tartozó szolgáltatások folyamatosságának biztosítása érdekében. A Bizottság a program kialakításakor javaslatot tesz az adatbázisok minimális tartalmára és formájára, valamint az összekapcsolásuk módjára vonatkozóan. A kritikus infrastruktúrák tulajdonosainak és üzemeltetőinek feladata a biztonsági tervek tényleges megvalósítása, valamint rendszeres ellenőrzések, gyakorlatok, felmérések és tervek végrehajtása révén a biztonság garantálása. A tagállamok ellenőriznék a folyamatokat, míg a Bizottság megfelelő ügyeleti rendszerek segítségével az egységes végrehajtást biztosítaná Unió-szerte. [50]

Az EPCIP azonban nem foglalkozik kiemelten a kritikus információs infrastruktúrák védelmével.

Az EPCIP vonatkozásában létrehoznák a *Kritikus Infrastruktúra Figyelmeztető Információs Hálózatot*[61] (a továbbiakban: CIWIN), melynek célja a tagállamok, EU intézmények, kritikus infrastruktúrák tulajdonosai és operátorai közötti, a közös fenyegetettségek, sérülékenységek és a kockázatcsökkentés érdekében megfelelő eljárások és stratégiák megosztására vonatkozó információcsere elősegítése és biztosítása.

A Bizottság javasolja egy olyan CIWIN hálózat kialakítását, amely azzal ösztönzi a megfelelő védelmi intézkedések létrehozását, hogy elősegíti a legjobb gyakorlat megismertetését, illetve eszközül szolgál az azonnali fenyegetések és riasztások továbbításában. A rendszer biztosítja, hogy a megfelelő személy a megfelelő információt kapja meg a megfelelő időben. [100]

A Bizottság szerint a következő három változatban képzelhető el a CIWIN hálózat fejlesztése:

1. A CIWIN egyfajta fórum, amelyen a kritikus infrastruktúrák védelemmel kapcsolatos ötleteket és legjobb gyakorlatot cserélik ki egymással a kritikus infrastruktúra tulajdonosok és üzemeltetők. Ez a fórum lehet szakértői hálózat és biztonságos

[61] Critical Inrastructure Warning Information Network (CIWIN)

elektronikus platform a vonatkozó információk cseréjéhez. A Bizottság fontos szerepet játszik az ilyen információ összegyűjtésében és terjesztésében. Ez a megoldás nem biztosítja a szükséges gyors riasztást az azonnali fenyegetések láttán. Ugyanakkor azonban lenne lehetőség a CIWIN bővítésére a jövőben.

2. A CIWIN egy gyorsriasztási rendszer (RAS), amely összeköti a tagállamokat a Bizottsággal. Ez a megoldás növeli a kritikus infrastruktúra biztonságát, mivel csak az azonnali fenyegetésekre biztosítana riasztást. A cél biztosítani a gyors információcserét a kritikus infrastruktúra tulajdonosokat és üzemeltetőket érintő potenciális fenyegetésekkel kapcsolatban. A RAS nem foglalkozik a hosszú távú hírszerzési információk terjesztésével. Ez a rendszer a konkrét infrastruktúrát érintő azonnali fenyegetésekre vonatkozó információk gyors terjesztésére szolgál.
3. A CIWIN egy többszintű kommunikációs/riasztó rendszer, amely két különböző funkcióból áll:
   a) gyorsriasztási rendszer (RAS), amely összeköti a tagállamokat a Bizottsággal;
   b) fórum a kritikus infrastruktúrák védelemmel kapcsolatos ötletek és legjobb gyakorlat kölcsönös cseréjére, amely a kritikus infrastruktúra tulajdonosoknak és üzemeltetőknek nyújt segítséget. Ez a megoldás egy szakértői hálózatból és egy elektronikus adatcsere platformból áll.

Ezért a Bizottság javasolja, hogy a kritikus infrastruktúra erősítése az Európai Unióban a közös EPCIP program kereteinek létrehozásával (közös célok és módszerek, pl. összehasonlításhoz, összefüggések), illetve a legjobb ágazati gyakorlat és a megfelelésre vonatkozó ellenőrző (monitoring) mechanizmusok cseréjével kezdődjön. A *Zöld Könyv* szerint a közös keretet alkotó elemek között kell említeni a következőket [100] :

- közös kritikus infrastruktúrák védelmi alapelvek;
- közösen elfogadott kódok és szabványok;
- közös meghatározások, amelyek alapján szektor-specifikus meghatározásokat lehet elfogadni;
- a kritikus infrastruktúra ágazatok közös listája;
- elsőbbséget élvező kritikus infrastruktúra védelmi területek;
- az érintett felelősök feladatainak leírása;
- elfogadott tesztek;
- módszerek az infrastruktúra összehasonlításához és rangsorolásához a különböző szektorokban.

A fenti ajánlásokból a kiemelendő a veszélyhelyzeti felkészülés kérdésköre. Ezt a munkát, amelyet alapvetően hazánkban a Kormányzati Koordinációs Bizottság lát el, nagyban elősegíthetné a fenti legjobb gyakorlatok hazai bemutatása és meghonosítása, valamint a szolgáltatók számára történő tudatosítása.

További fontos ajánlás a kritikus infrastruktúrával kapcsolatos információ-megosztás, amely jelenleg a hírközlési ágazat tekintetében az Országos Informatikai és Hírközlési Főügyelet, valamint a vele szoros együttműködésben működő CERT Hungary központ lát el. Ez a rendszer mindenképpen alkalmassá tehető a fenti ajánlás megvalósítására megfelelő fejlesztések végrehajtása (pl. CIWIN hálózathoz történő csatlakozás, hazai és EU szintű ügyeleti rendszerhez történő csatlakozás/együttműködési megállapodások létrehozása, stb) után.

Ennek az ajánlásnak a megvalósításában a Bizottság képviselői szerint az EU hálózatbiztonsági szervezetének, az ENISA-nak jelentős szerepet kell betöltenie. Szintén feladatként jelentkezik az infrastruktúrák közötti függőségek feltárása, amely az EPCIP program keretében kizárólag a két-, vagy több tagállamot érintő infrastruktúrákat érinti, ugyanakkor ennek hazai rendszerét is szükségszerűen ki kell dolgozni, illetve kezdeményezni kell a megfelelő jogi háttér megteremtését. A nyilvános hálózatok prioritási rendszerének biztosítása, bár több nemzetközi szervezet ajánlása tartalmazza azokat, illetve más országok gyakorlatába is beépült, itthon kevés figyelmet kapott. Ezt a rendszert minimális átalakítással és költségráfordítással az infokommunikációs szolgáltatók be tudnák építeni rendszereikbe, amely által egy katasztrófa-, illetve válsághelyzet során az érintettek közötti vitális válsághelyzeti kommunikáció feltételei biztosíthatóak lennének.

A Bizottság által javasolt lépések a következők:

- magánszektorral történő kapcsolatfelvétel, különösen az interdependenciák vizsgálatával;
- kutatás, modellezés;
- szabályozási kérdések rendezése;
- kritikus infrastruktúrák védelmi kontaktpontok ágazati szintű kijelölése.

A Bizottság elképzelései szerint a szektor specifikus kritikus infrastruktúra kritériumok meghatározását követően a tagállamoknak egy évük van azok azonosítására, majd újabb egy év múlva el kell készíteniük az azokra vonatkozó biztonsági terveket. Ezt a tevékenységet a magánszférával szoros együttműködésben kell végezni, különös tekintettel arra, hogy a kritikus infrastruktúra üzemeltetőinél egy kapcsolattartó személy válik szükségessé.

A kritikus infrastruktúra feladatainak forrásául szolgálnak a Bizottság Joint Research Centerének kezdeményezései, a 7-es keretprogramban az EU Biztonság és Űr (Security and Space) programjára elkülönített 140 millió euró, valamint a Bizottság által jóváhagyott 150 millió euró, amely összeg a biztonsági kutatásokra fordítható. Ezek a források részben a DG Finance-szel közös tenderkiírások keretében készíti elő a DG INFSO.

A 2007-2008-as időszakra a DG INFSO egy újabb tanulmány elkészítését finanszírozza meg, amely az EU szintű kritikus infrastruktúrák egymástól való függését hivatott azonosítani, és amelyben a tagállamok, a nemzeti szakértők részvételére, aktív részvételére is számítanak. További feladatként jelentkezik a helyi szintű kritikus infrastruktúrák védelmi, kritikus információs infrastruktúrák védelmi tevékenység felmérése és nemzeti szintű szabályozás kereteinek kimunkálása, amelyre az EPCIP is ráépülhet. Formálisabb egyeztetési mechanizmus kidolgozását 2008-ra ígérte a DG INFSO.

A Megbízható Fejlődést Támogató Kezdeményezés

Az Európai Unió 2001 júniusában életre hívta a kritikus infrastruktúrák információs biztonságáért a *Megbízható Fejlődést Támogató Kezdeményezést*[62] (a továbbiakban: DDSI). A másfél éves *Információs Társadalmi Technológiák Projekt* egy, a kritikus infrastruktúrák függőségének szabályozását célzó terv fejlesztését tűzte ki célul az akkori 15 tagállam részére. [52]

A DDSI az EU tagállamok, és egyes kiválasztott unión kívüli államok kritikus infrastruktúrájának sérülékenységeit vizsgálva megállapította, hogy a kritikus infrastruktúrák iránti tudatosság növekedett Európában; ugyanakkor az államok felkészültségének szintje eltérő, sok a lemaradás; a kritikus infrastruktúrák fenyegetettsége az internet támadások számának gyors növekedését követi. A kialakított akcióterv az EU, a nemzetek és a magán ipar közötti együttműködést célozta meg, melyben minden félnek megvan a maga felelősségi területe.

Megállapításai:

- A **magánipar** részére:
  - fejlessze az információs biztonság menedzselését;
  - alkalmazzon új biztonsági technológiákat;
  - fejlesszen ki olyan biztosítási és befektetési eszközöket, amelyek a jó biztonsági gyakorlatokat segítik.

[62] Dependability Development Support Initiative

- A **nemzeti kormányzatok** részére:
  - EU tagállamok egymás közötti jogharmonizációja a számítógépes bűncselekmények vonatkozásában;
  - Nemzeti hálózatbiztonsági intézmények és rendszerek európai vagy globális szintű szabványokhoz igazítása, alkalmazása. A projekt olyan biztonsági és kockázatelemzési[63] szabványok alkalmazását javasolta, mint például az *ISO 17799* vagy az *OECD információbiztonsági irányelvei*.

E folyamatban az EU szerepét elsősorban a felek közötti partneri viszony kiépítésében, kapcsolatok kialakításában, az információbiztonsági közpolitika szabályozásában és ajánlásokban, információcsere támogatásában látta. [53]

Az Európai Hálózati és Informatikai Biztonsági Ügynökség

Az EU Bizottság az Európai Hálózat- és Informatikai Biztonsági Ügynökség[64] (a továbbiakban ENISA) létrehozására irányuló javaslatában [92] a Bizottság kijelentette, hogy a hálózati és információbiztonság nagy politikai jelentőségre tett szert. 2004-ben az Európai Parlament és Tanács rendeletével [19] ötéves időtartamra létrehozták az Európai Hálózat- és Informatikai Biztonsági Ügynökséget. Az ENISA létrehozásának fő célja *„A Közösségen belüli magas szintű és hatékony hálózat- és információbiztonság biztosítása, valamint az Európai Unió polgárai, fogyasztói, vállalkozásai és a közszektor szervezetei érdekében a hálózat- és információbiztonság kultúrájának kifejlesztése céljából, és ezáltal elősegítve a belső piac zavartalan működését, létrehozza az Európai Hálózat- és Információbiztonsági Ügynökséget”* [19].

ENISA mind a tagállamok, mind az EU-intézményei számára szakértői központként működik, amely hálózati és információs biztonsági kérdésekben tanáccsal látja el a hozzáforduló szervezeteket. Ebben a minőségében az ENISA támogatja a tagállamok, az EU-intézmények és a vállalkozások azon képességének megerősítését, amely a hálózati és információs biztonsági problémák megelőzésére és kezelésére irányulnak. Az ENISA a tervek szerint olyan tudásközpont lesz, amelynek segítségét a tagországok és az uniós intézmények is

[63] A javasolt anyagok egyike sem tartalmaz a kockázatelemzésre felhasználható leírást, csak a kockázatelemzéshez kiindulási „elvárásként” szolgálnak.

[64] European Network and Information Security Agency (ENISA)

igénybe vehetik az infokommunikációs biztonság területén felmerülő problémáik megoldásában.

Az ENISA feladatai:

- megfelelő információk gyűjtése a jelenlegi és a jövőbeli kockázatok elemzése céljából, különös tekintettel azokra az információkra, melyek hatással lehetnek az elektronikus hírközlő hálózatok terhelhetőségére, továbbá az említett információk hitelességére, sértetlenségére és bizalmasságára;
- a hálózat- és információbiztonsággal kapcsolatos problémák megelőzésére szolgáló *közös módszerek* kidolgozása;
- a tudatosság növeléséhez való hozzájárulás; a *mindenkori legjobb gyakorlatok* cseréjének és a *figyelmeztetésre szolgáló módszereknek* az ösztönzése;
- a kockázatértékelési és irányítási tevékenységek előmozdítása;
- a hálózat- és információbiztonság területén működő különböző szereplők közötti együttműködés fokozása;
- segítségnyújtás a Bizottságnak és a tagállamoknak a hardver- és szoftvertermékek biztonságával kapcsolatos problémák megoldása érdekében az iparral folytatott párbeszédben;
- a harmadik országokkal, illetve adott esetben nemzetközi szervezetekkel folytatott közösségi erőfeszítésekhez való hozzájárulás a hálózat- és információbiztonsággal kapcsolatos kérdésekre vonatkozó egységes globális szemlélet ösztönzése érdekében, hozzájárulva ezáltal a hálózat- és információbiztonság kultúrájának kifejlesztéséhez.

Az 1990-es évek végétől az európai tagállamok fokozatosan különböző operatív és jogi szervezeteket alakítottak ki a kritikus infrastruktúrák hatékonyabb védelme, és a hálózatok elleni támadások megfelelőbb reagálása érdekében. [56]. Ezek a szervezetek az alábbi három kategóriába sorolhatók:

- Számítógépes Vészhelyzeti Reagáló Csoportok[65] és Számítógépes Biztonsági Incidens Reagáló Csoportok[66];
- Számítógépes Bűnügyi Egységek[67];
- egyéb speciális szervek.

[65] Computer Emergency Response Team (CERT)

[66] Computer Security Incident Response Team (CSIRT)

[67] Computer Crime Unit (CCU)

2.2.2.2. A NATO

A NATO Polgári Vészhelyzeti Tervezés[68] 2005-2006 időszakára kiadott miniszteri irányelvek már számos utalást adnak a kritikus infrastruktúrák védelmére.

A Polgári Vészhelyzeti Tervező Bizottság[69] (a továbbiakban: SCEPC) egyetértett abban, hogy folytatni kell a tagállamok felkészülését a kritikus infrastruktúrákat ért esetleges terrortámadásokra. Az SCEPC nyolc tervező csoportot és bizottságot[70] hozott létre, hogy funkcionális szempontból vizsgálják a kritikus infrastruktúrák védelmét, amely során egységes szakértelemmel támogassák minden területen a bizottságokat.

Civil Kommunikáció Tervező Bizottság[71]

A bizottság feladata a meglévő és tervezett kommunikációs rendszerek, berendezések, szolgáltatások vizsgálata, amely kiterjed arra, hogy ezek megfelelnek-e a civil, illetve katonai követelményeknek veszélyhelyzet esetén.

A bizottság közreműködött az Észak-atlanti Tanács kibervédelmi tervének (North Atlantic Council's Action Plan on Cyber Defense) kidolgozásában is. Ebben a munkában vizsgálták az információs hadviselés és a kibertámadások hatásait a civil kommunikációs rendszerekre. Megvizsgálták, hogy egy ilyen esetben milyen szerepet kaphatnának a CERT-ek. Elemezték a kritikus infrastruktúrák és a civil kommunikációs rendszerek interdependenciáját (egymásra utaltságát és összefüggéseit).

Polgári Védelmi Bizottság[72]

A bizottság 2001-ben egy ad-hoc csoportot hozott létre a kritikus infrastruktúrák védelmének kérdéseit vizsgálandó. A csoport első feladata az volt, hogy felmérje és meghatározza a kritikus infrastruktúrákat. A munkába meghívták és bevonták a tagállamok képviselőit is. A munka eredménye a Kritikus Infrastruktúrák Védelem Koncepcionális Tanulmány volt (Critical Infrastructure Protection – Concept Paper), amelyet 2003-ban publikáltak.

---

[68] NATO Civil Emergency Planning (CEP)

[69] Senior Civil Emergency Planning Committee (SCEPC)

[70] Planning Boards and Committees (PB&Cs)

[71] Civil Communication Planning Committee (CCPC)

[72] Civil Protection Committee (CPC)

Ipari Tervező Bizottság[73]

Ez a bizottság az ipari és kereskedelmi infrastruktúrák interdependencián alapuló sérülékenységét, és az azokra adható megoldásokat vizsgálja.

Élelmiszer és Agrár Tervező Bizottság[74]

A bizottság fő feladata annak vizsgálata, hogy a kritikus infrastruktúrák milyen hatással vannak az élelmiszer előállítására, az agráriparra, valamint az ivóvíz ellátásra. Áttekintik a veszélyeket, kihívásokat, sebezhető pontokat.

Polgári Repülés Tervező Bizottság[75]

A bizottság feladata a – egyébként nemzeti hatáskörben lévő – polgári légi közlekedés számára úgynevezett minimum standardok kidolgozása.

Közúti Szállítások Tervező Csoportja[76]

A csoport feladata annak vizsgálata, hogy a szárazföldi szállításokra milyen hatással lehet egy esetleges – az úthálózatot ért – támadás. A csoport célja felmérni melyek a legvalószínűbb célpontok, valamint milyen védelmi megoldásokkal lehet ezek biztonságát növelni, illetve a támadásokat megelőzni.

Tengeri Hajózás Tervező Csoport[77]

A csoport tanácsadó és közreműködő szerepet tölt be a polgári tengeri hajózás terrorizmus elleni küzdelmében. Feladata a különböző nemzetközi testületek munkájának monitorozása, elemzése, információgyűjtés és -csere különböző nemzetközi és nemzeti forrásokból, valamint tanácsadás biztosítása.

Koordináció

A kritikus infrastruktúrák védelmi munkái koordinációjáért a SCEPC felelős. Ugyanakkor a bizottságok képviselői rendszeresen tanácskozásokat tartanak a kérdésben. Ezeken a tanácskozásokon a bizottságok beszámolnak az elvégzett és az előttük álló munkáról, valamint döntenek a bizottságok közötti koordinációs és együttműködési kérdésekről is.

[73] Industrial Planning Committee (IPC)

[74] Food and Agriculture Planning Committee (FAPC)

[75] Civil Aviation Planning Committee (CAPC)

[76] Planning Board for Inland Surface Transportation (PBIST)

[77] Planning Board for Ocean Shipping (PBOS)

2.2.2.3. Nemzetközi szervezetek

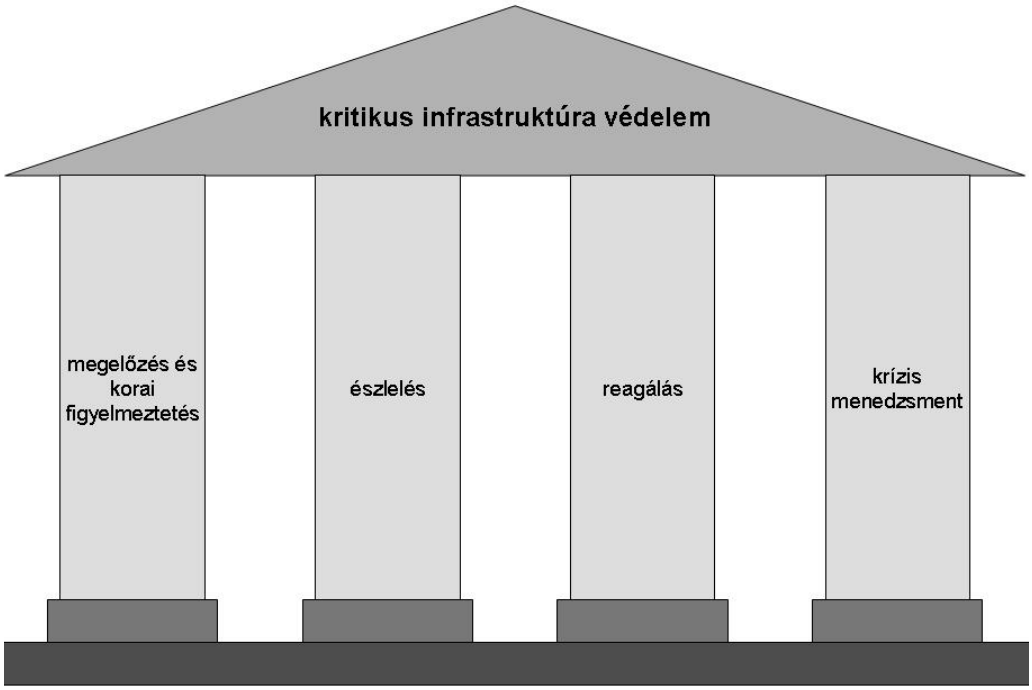
Számítógépes Vészhelyzeti Reagáló Csoportok és Számítógépes Biztonsági Incidens Reagáló Csoportok

A Számítógépes Vészhelyzeti Reagáló Csoportok és Számítógépes Biztonsági Incidensek Reagáló Csoportok (a továbbiakban: CERT, CSIRT) a köz- vagy magánszféra technikai csoportjai, akik figyelnek, figyelmeztetnek, és támadásokra reagálnak.

Az EuroCERT projekt keretében 1999-2000-ben megkísérelték az európai monitoring és figyelmeztető tevékenységek koordinációját, de ezt a már létező CERT-ek közössége nem fogadta el. Azóta a tudományos, kormányzati vagy kereskedelmi státusszal bíró specializálódott csoportok száma a legtöbb tagállamban növekedett. 2006 májusában 89 CSIRT működött Európa 30 államában, közülük 49-et akkreditált a TF-CSIRT[78], mely akadémiai koordinációs szervezetként képzésben, szabványosításban (incidensek kategorizálása) és biztonsági linkek területén bocsát ki kezdeményezéseket, és különös hangsúlyt helyez monitoring és figyelmeztető források kis és középvállalkozások általi elérhetőségére.

Számos tagállamban – köztük Magyarországon is – találhatunk kormányzati CERT-et, melyek feladata elsősorban az állami információs rendszerek elleni támadásokra történő reagálás. A CERT-ek fontosságára rámutat az a tény is, hogy a szakértők véleménye szerint a kritikus információs infrastruktúrák védelmének magvalósítása a megelőzés és korai figyelmeztetés, az észlelés, a reagálás és a krízismenedzsment négy pillérén kell, hogy alapuljon. Ezt a négy pillért mutatja be a 4. ábra. Ezeknek a feladatoknak egy jelentős részét elvégzik a CERT-ek, valamint a krízismenedzsmenthez is hatékony segítséget tudnak nyújtani.

[78] A TF-CSIRT Munkacsoportot a TERENA (Transz-Európai Kutató és Oktatási Hálózat Társaság) égisze alatt hozták létre az európai CSIRT-ek közötti együttműködés elősegítésére.



4. ábra – A kritikus infrastruktúrák védelem négy alappillére [96]

A Európai Bizottság álláspontja szerint a nemzeti kritikus infrastruktúrák védelmi kontaktpontokból álló kritikus infrastruktúrák védelmi kontaktcsoportnak – mint stratégiai koordinációs és együttműködési platformnak – kettős rendeltetése van: egyrészt a nemzeti kritikus infrastruktúrák védelmi kapcsolati pontok delegálnak képviselőt az ECI[79]-irányelv végrehajtását elősegítő komitológiai bizottságba, vagyis a kritikus infrastruktúrák védelmi kontaktcsoport egy részről komitológiai bizottságként funkcionál, másrészt a negyedéves ülések során lehetőség nyílik az informális párbeszédre, a legjobb gyakorlatok, releváns tanulmányok eredményének megosztására.

Mindezek alapján arra a következtetésre jutottam, hogy a kritikus infrastruktúrák védelmi kontaktpont nem veszi át az ágazati kritikus infrastruktúrák védelmi kompetenciákat. **A kritikus infrastruktúrák védelmi kapcsolati pont tagállamon belüli koordinációs tevékenysége az ECI-irányelvben foglalt – EU kritikus infrastruktúrák védelmi – kötelezettségek nemzeti koordinációjára vonatkozik, nem pedig a nemzeti kritikus infrastruktúrák védelem koordinációjára!**

[79] European Critical Infrastructure, európai kritikus infrastruktúra

Számítógépes Bűnügyi Egységek

A Számítógépes Bűnügyi Egységek[80] (CCU) az infokommunikációs technológiák használatával kapcsolatos bűncselekmények felderítésében vesznek részt.

A számítógépes bűncselekmények felderítésére specializálódott egységek feladata a hálózatokat ért támadások esetén büntetőeljárások lefolytatása. Ebben a munkájukban a hazai CERT-ek, illetve a CSIRT-ek technikai szakértelmére támaszkodhatnak. A gyakorlatban azonban feladataik többsége leginkább olyan, hagyományos bűncselekményekre terjed ki, ahol az információs rendszereket elkövetés eszközéül használták. Tulajdonképpen ebben az esetekben csak háttércsapatként szolgálnak a hagyományos nyomozati szerveknek. Ezen egységek létszáma kevés a feladathoz mérten, a tevékenységük jó része más nyomozati szervek tevékenységének koordinálásban merül ki. Csak néhányuk rendelkezik saját megfigyelő hálózattal.

Az Egyesült Királyságban a Nemzeti Fejlett Technológiai Bűnüldözési Egység[81], az NHTCU, mint nemzeti szervezet kapcsolatokat biztosít a helyi szervezetek között az országban, illetve együttműködést az ügynökségekkel, és kapcsolódik az iparágak képviselőihez.

Franciaországban a belügyminisztériumon belül 2000 májusában létrehozott Információs és Kommunikációs Technológiákhoz Kötődő Bűnözés Elleni Harc Központi Hivatala[82], az OCLCTIC látja el a magas technikai ismereteket igénylő bűnügyek kezelését, a számítógépes bűncselekményekre szakosodott regionális nyomozók képzését, illetve Nemzeti Kontakt Pontként jelentkezik a nemzetközi szervezetek (Europol, Interpol, G-8) számára.

Összességében ezeknek a nemzeti specializálódott bűnüldöző csoportoknak még belső növekedésre, az információs biztonsággal foglalkozó más nemzeti szervekkel való kooperációra, illetve a határokon átnyúló ügyek kezelése érdekében más országok hasonló szervezeteivel való együttműködésre van szükségük a hatékony működés érdekében.

[80] Computer Crime Units (CCU)

[81] National High Technology Crime Unit - NHTCU

[82] Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication - OCLCTIC

Kritikus Információs Infrastruktúra Fejlesztési Koordináció

A Kritikus Információs Infrastruktúra Fejlesztési Koordináció[83] (CI2RCO) az Európai Unió támogatásával, az Információs Társadalom Technológiái[84] égisze alatt létrejött kritikus információs infrastruktúrák védelem fejlesztési és koordinációs projekt. Jelenleg az alábbi szervezetek vesznek részt a munkában:

- Fraunhofer Institute for Secure Information Technology – Németország;
- Ernst Basler & Partner – Svájc;
- Italian National Agency for New Technologies, Energy and the Environment – Olaszország;
- Ecole Nationale Supérieure des Télécommunications – Franciaország;
- Industrieanlagen-Betriebsgesellschaft mbh – Németország;
- Project Management Organisation in the German Aerospace Center (DLR) – Németország;
- The Netherlands Organisation for Applied Scientific Research – Hollandia;
- Cityplan Ltd. – Csehország;
- The Institute of Control Systems – Lengyelország.

A kritikus információs infrastruktúrák védelmére szakosodott nemzetközi szervezetek a következők:

- **International Watch and Warning Network (IWWN)**: Tagjai a legfejlettebb gazdasággal rendelkező államok (pl.: USA, Japán, Németország, Hollandia, stb.), valamint Magyarország. A szervezet célja, hogy minden tagországból közös fórumot biztosítson a nemzetgazdaságot érintő kockázatok kezelésben a jogszabályalkotóknak, a kormányzati CERT szervezeteknek, valamint a bűnüldözési szervezeteknek.
- **TF-CSIRT:** A TF-CSIRT az Európában működő CERT-ek közös szervezete, amelynek célja a CERT-ek közötti információcsere hatékony biztosítása, valamint a globális fenyegetésekkel szembeni közös fellépés elősegítése.
- **Forum of Incident Response Teams (FIRST):** A FIRST a CERT-ek világszervezete, amelynek célja a CERT-ek együttműködésének elősegítése globális szinten, valamint a globális fenyegetésekkel szembeni közös fellépés megteremtése.

[83] Critical Information Infrastructure Research Co-ordination (CI2RCO)

[84] Information Society Technologies (IST)

- **European Governmental CERTs (EGC):** Az EGC szervezet a vezető európai uniós államok kormányzati CERT-jeinek szoros együttműködését tűzte ki célul, és jelenleg 7 tagja van (pl. Németország, Franciaország, Finnország, Hollandia).

2.2.2.4. Nemzeti szervezetek

Az **Egyesült Államok** esetében a hálózatbiztonság szinte minden aspektusban érinti a kritikus infrastruktúrák védelmét. A legtöbb amerikai vállalkozás már nem képes a hálózati működését fizikai működésétől elválasztani, mert azok annyira összekapcsolódtak.

Az 1998-as, Clinton adminisztráció meghatározó elképzelése volt a nemzeti infrastruktúrák védelem vonatkozásában a magánszektor erőteljes bevonása. A 63. számú Elnöki Direktíva tette lehetővé az Információ Megosztó és Elemző Központok[85] létrehozását a magánszektor és a szövetségi kormányzat között, a nemzeti kritikus infrastruktúrákra vonatkozó együttműködés és információcsere erősítése érdekében.

Az Információ Megosztó és Elemző Központok (ISAC) feladata az adott szektor kritikus infrastruktúráinak fenyegetettségeinek és sérülékenységeikre vonatkozó lényeges információk továbbítása a szövetségi kormányzat részére.

Jelenleg ilyen elemző és információmegosztó központ működik az élelmiszeriparban, a víz- és energiaszektorban, továbbá az információs technológia, telekommunikáció, kémiai és pénzügyi szolgáltató szektorban.

A működésükkel kapcsolatban problémát jelent a központok fenntartási költsége, mely egyoldalúan az ipari szektorokat terheli.

Az amerikai nemzetbiztonsági stratégia a fenti elgondolás mentén kettéválasztja a fizikai és elektronikus biztonságot. A *National Strategy for Homeland Security* elkülönült részét képezi a hálózatbiztonsági nemzeti stratégia, a *National Strategy to Secure Cyberspace*, illetve a kritikus infrastruktúra fizikai védelmének koncepcióját meghatározó *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.*

A 2002-ben létrehozott Belbiztonsági Minisztérium[86] az egyik kulcsintézmény a nemzeti kritikus infrastruktúrák védelmi stratégiájának és az elektronikus védelmi stratégia megvalósításában. E szerepében elsősorban a következőképp összefoglalható feladatokat lát el:

[85] Information Sharing and Analysis Centre (ISAC)

[86] Department of Homeland Security (DHS)

- szövetségi, állami, önkormányzati és magánszektor koordinációja és integrációja;
- nemzeti infrastruktúrák védelmi terv készítése és a sérülékenységek fenyegetettségeinek feltérképezése, valamint figyelmeztetések kibocsátása. Azonban míg az infrastruktúrák fizikai védelmén más szervezetekkel együttműködik, az elektronikus biztonság területén egyeduralkodó szerepet tölt be.
- nemzeti elektronikus hálózatbiztonsági stratégiában foglaltak megvalósítása.

Az amerikai elektronikus hálózatbiztonsági stratégia öt nemzeti prioritást állapított meg:

1. prioritás: **nemzeti hálózatbiztonsági reagáló rendszer kialakítása,** az állami reagáló képesség és a bekövetkező károk csökkentése érdekében;
2. prioritás: a **nemzeti hálózatbiztonsági fenyegetettségek és sérülékenységek csökkentését célzó program** kialakítása;
3. prioritás: ugyanezen célból **nemzeti hálózatbiztonsági tudatossági és tréning program** kialakítása;
4. prioritás: a **kormányzati hálózatbiztonság**;
5. prioritás: nemzeti biztonsági és nemzetközi **hálózatbiztonsági együttműködés** kialakítása.

A feladatok végrehajtására 2003 júniusában létrehozták a Nemzeti Hálózatbiztonsági Főigazgatóságot[87] (NCSD). Az NCSD folyamatos a nap 24 órájában, a hét minden napján működik, feladata hálózatbiztonsági elemzések végzése, figyelmeztetések és felhívások kibocsátása, az információ áramlás elősegítése, nagyobb incidensekre reagálás, valamint a nemzeti szintű helyreállítás elősegítése.

A 60 fővel működő Főigazgatóság három fő célkitűzés mentén szerveződött:

- **Általános hálózati feladatok**: segítségnyújtás a kormányzati hálózati eszközök sérülékenységének csökkentéséhez, kockázatok meghatározása, magánszektor koordinálása a nemzeti kritikus információs elemek beazonosításában és védelmében.
- **Felügyelet és koordináció**: A Hálózatbiztonsági Követő, Elemző és Reagáló Központ (CSTARC) felügyelete, melynek feladata az internetes események nyomozása, és megoldása, potenciális hálózati fenyegetettségek és sérülékenységek követése; a magánszektor, a helyi, állami és szövetségi szervek, valamint nemzetközi szervek

[87] National Cyber Security Division (NCSD)

között a hálózatbiztonság és incidens reagálás koordinálása.

- **Megelőzés, képzés**: más szervekkel együttműködve hálózatbiztonsági tudatossági és képzési programok kialakítása, partneri együttműködés fogyasztókkal, vállalkozásokkal.

Az NCSD szorosan együttműködik:

- a Nemzeti Szabványügyi és Technológiai Intézettel[88];
- a szövetségi rendvédelmi szervekkel;
- a nemzetbiztonsági szervekkel;
- az adatvédelmi megbízottal;
- a tudományos és technológiai szervezetekkel.

Emellett 2004 novemberében a Belbiztonsági Minisztérium Információ Elemző és Infrastruktúrák Védelmi Főigazgatóságán belül is megalakult a Nemzeti Cyberbiztonsági Főosztály, melynek főosztályvezetője felelős a minisztérium valamennyi hálózatbiztonságot érintő kritikus infrastruktúrák védelmi programért.

E főosztály feladata többek között:

- a nemzeti kritikus infrastruktúrára kiható hálózatbiztonsági fenyegetéseket és sérülékenységeket csökkentő program kialakítása;
- együttműködés az amerikai katasztrófavédelemmel abból a célból, hogy a nemzeti helyreállítási terv tartalmazza a kritikus infrastruktúrák hálózatbiztonsági elemeinek visszaállítására vonatkozó megfelelő eljárásokat;
- nemzeti és nemzetközi együttműködési program megvalósítása.

Az Egyesült Államok mintáját követve az európai kormányok kritikus infrastruktúrájuk és kapcsolódó információs rendszerek védelmére kifejezetten specializálódott szervezeteket is létrehoztak. A következőkben ezeknek a szervezeteknek az elhelyezkedését, és feladataikat vizsgálom meg az Egyesült Királyság, Németország és Franciaország területén.

Az **Egyesült Királyságban** a létfontosságú nemzeti infrastruktúrák információs biztonságának megteremtésére egy tárcaközi központot hoztak létre.

[88] National Institute of Standards and Technology (NIST)

Az 1999 óta fennálló Nemzeti Infrastruktúrák Biztonsági Koordinációs Központ[89], a NISCC működésében a kabinet hivatala, a CESG[90], a DSTL[91], a belügyi, az ipari és kereskedelmi tárcák, a védelmi minisztérium, a Nemzeti Hi-Tech Bűnözési Egység (National Hi-Tech Crime Unit[92]) és a nemzetbiztonsági szolgálattal működik együtt.

A 85 munkatársat alkalmazó szervezet működéséhez szükséges anyagi forrásokhoz az Egyesített Incidens Jelentő és Figyelmeztető Sémán, az UNIRAS[93]-on (kormányzati CERT) keresztül jut. A Központ 2005/2006. évi költségvetése közel 10 millió angol font volt.

Az Egyesült Királyság sajátossága, hogy kritikus infrastruktúrái többsége magánkézben összpontosul. Ennek megfelelően a NISCC számos céggel működik szorosan együtt. Az együttműködő cégek egy része külföldi tulajdonban áll, vagy erős nemzetközi kötődése van. Ennek következtében a létfontosságú nemzeti infrastruktúrákhoz kötődő ügyek átlépik a földrajzi országhatárokat. Mivel problémáik a világ bármely részén jelentkezhetnek, a NISCC globális feladatrendszerrel működik.

A NISCC felelőssége az Egyesült Királyság kritikus infrastruktúrájának elektronikus támadásokból eredő kockázatának csökkentése.

A szervezet nem normaalkotó, szabályzó vagy rendvédelmi jellegű; a kritikus infrastruktúrák operátorai számára technikai tanácsot, fenyegetettségekkel, sérülékenységekkel kapcsolatos információt és figyelmeztetéseket ad.

Feladatait négy alapvető kategóriában sorolja:

- **Fenyegetettség-elemzés**, azaz fenyegetettségek felderítése, értékelése és megszüntetése.
- **Fejlesztés**, azaz védelem és biztonság elősegítése kölcsönös információ-megosztás támogatásával, illetve tanácsadással és a legjobb gyakorlat támogatásával.

---

[89] National Infrastructure Security Coordiantion Centre (NISCC)

[90] Az Egyesült Királyság kormányának információbiztonságért felelős nemzeti technikai hatósága

[91] Defence Science and Technology Laboratory, (Védelmi Tudományos és Technológiai Laboratórium), az angol védelmi minisztérium kutatási központjai, mely egyben az egyik legtöbb kutatót és mérnököt tömörítő szervezet az angol közszférában.

[92] A National Hi-Tech Crime Unit 2001 áprilisában alakult a National Crime Squad részeként. Feladata az Egyesült Királyságot is érintő súlyos és szervezett hi-tech bűncselekmények felderítése, függetlenül elkövetési helyétől. Jellegzetessége, hogy munkatársai a különböző rendvédelmi szervektől delegálják, többek között a National Crime Squad (NCS), a National Criminal Intelligence Service (NCIS), Her Majesty's Customs and Excise Law Enforcement Investigation (HMC&E), a nemzetbiztonsági hivatalok és a hadsereg.

[93] Unified Incident Reporting and Alert Scheme

- **Reagálás**, azaz az új veszélyekre való figyelmeztetés, elhárításra vonatkozó tanácsadás, sérülékenységek közzétételének menedzselése, segítségnyújtás a nemzeti kritikus infrastruktúráknak nyomozásokban és támadások utáni helyreállításban.
- **Kutatás, fejlesztés**, azaz valamennyi kategória tevékenységének támogatásához a leghaladóbb technikák és metódusok kidolgozása.

A NISCC információ megosztó stratégiájának részeként a figyelmeztetések rögzítését és az incidensek jelentését (beavatkozási jog nélkül) a WARP[94] végzi. A figyelmeztetésekről és incidensekről szóló információk terjesztésében (általában kereskedelmi alapon) szintén egy másik szervezettel, az ISAC[95]-kal működik együtt.

Jelenleg éles politikai vita folyik arról, hogy a brit kormányzat létrehozzon-e szabványokat a kritikus infrastruktúra elemeinek tervezéséhez és üzemeltetéséhez, illetve a üzemeltetéséhez kialakítson-e minősítő rendszert. Egyes politikai elképzelések tovább lépnek, és a kritikus infrastruktúrák infokommunikációs biztonságának minimum feltételét egy – a megfelelőség biztosításához és az alkalmasság ellenőrzéséhez szükséges – validációs rendszer létrehozásában látják. [1]

Németországban, 1999-ben a Szövetségi Belügyminisztériumban (BMI) megalakult az AG KRITIS[96] munkacsoport a kritikus infrastruktúrák védelmére. A munkacsoportban az IS 5 (fizika védelem), a PII 1 (fenyegetettség megelőzés) és az IT 3 (IT és IT függőség) szakértői vesznek részt. Emellett a Szövetségi Bűnügyi Rendőrség Hivatala (BKA) és a Szövetségi Katasztrófavédelem és Polgári Védelem Hivatala (BBK), valamint a Szövetségi Informatikai Biztonság Hivatala (BSI) szakértői is rendszeresen részt vesznek a munkában. Az MBI munkacsoport egyik feladata egy nemzeti terv kifejlesztése az infokommunikációtól függő kritikus infrastruktúrák védelmére.

A BSI a BMI égisze alatt rendkívül fontos szerepet játszik a kritikus infrastruktúrák védelmi programjában. A BSI kezeli szinte valamennyi, az információs társadalom biztonságához kapcsolódó területet. E munka során megelőző lépéseket tesz infokommunikációs gyengeségek elemzése és védelmi eljárások kidolgozása formájában, ideértve a következő területeket:

---

[94] Warning, Advice and Reporting Point /Figyelmeztető, Tanácsadó és Jelentő Pont

[95] Information Sharong and Analysis Centre / Információ Elosztó és Elemző Központ

[96] German Arbeitsgruppe Kritischer Infrastructuren / Német Kritikus Infrastruktúra Munkacsoport

- internet biztonság: elemzések, koncepciók, tanácsadás;
- vírusközpont és a CERT menedzselése;
- hálózatbiztonság és kriptográfia, nyilvános kulcsú infrastruktúra[97] és biometria;
- kritikus infrastruktúrák.

Németországban a kormányzat, a civil szerveztek, valamint a cégek közötti együttműködés (PPP[98]) jelentősnek tekinthető.

Ennek az együttműködésnek az a felismerés adta az alapját, hogy a kritikus infrastruktúrák hatékony védelme csak a köz- és magánszektor szoros együttműködésével valósulhat meg. Így számos civil-kormányzati kezdeményezés játszik szerepet a német kritikus infrastruktúrák védelmében.

Ezek közül példaként említhető a D21 Kezdeményezés, mely non-profit szervezetként több mint 300 céget tömörít magában különböző ágazatokból. A kezdeményezés célja, hogy a kormányzattal együttműködve felgyorsítsák Németország átmenetét az ipari társadalomból az információs társadalomba.

Meg kell említeni még az AKSIS[99] kormányzati és polgári infrastruktúrák védelmi munkacsoportot is, melynek célja a kritikus infrastruktúrák összekapcsolódásának elemzése volt, hangsúlyozva azok függőségét az információs technológiáktól. További céljuk a megelőzés, a válaszadás érdekében eljárások, és megfelelő biztonsági menedzsment kialakítása volt.

Franciaországban ez a feladat egyértelműen a nemzetvédelmi miniszter (SGDN) hatáskörébe van utalva, akinek a Nemzeti Információ Biztonsági Ügynökség (DCSSI) is alá van rendelve.

A védelem módszere egyrészt az érzékeny pontok és hálózatok országos szintű, rendszeres ellenőrzésén, másrészt éberségi és beavatkozási terveken alapul. A tervek az információs hálózatok fenyegetettségeit veszik számba, és rendszeres gyakorlatokat tartanak a teljes állami apparátus vagy annak egy meghatározott részei számára.

---

[97] public key infrastructure (PKI)

[98] A PPP (Public Private Partnership) a közfeladatok ellátásának az a módja, amikor az állam a szükséges létesítmények és/vagy intézmények létrehozásába, fenntartásába és üzemeltetésébe (versenyeztetés útján) bevonja a magánszektort.

[99] German Arbeitskreis Schutz kritischer Infrastrukturen (1997-2000)

A **bemutatott védelmi megoldásokból jól látható**, hogy a **kritikus információs infrastruktúrák védelme terén** – eddig – az **USA tette a legtöbbet**. Ennek egyik oka az, hogy itt a legfejlettebb az információs társadalom és a fejlett információs társadalom szükségszerűen a saját infrastruktúrái védelmére is nagy gondot fordít. Mindezek mellett a fokozott fenyegetés szintén hozzájárul, ahhoz, hogy itt találjuk a legfejlettebb védelmi megoldásokat mind jogszabályi, mind szervezeti szinten.

Az amerikaiak – szokásuk szerint – az ezzel kapcsolatos tanulmányokat, stratégiai terveket elhelyezik az interneten, így mindenki megismerheti azokat – és szívesen fogadják a javaslatokat, az építő kritikákat. Természetesen a megfelelő gazdasági háttér nagyban hozzájárul a védelem megteremtéséhez.

KÖVETKEZTETÉSEK

Megvizsgáltam és elemeztem a kritikus információs infrastruktúrákat fenyegető veszélyeket. Külön vizsgáltam a fizikai dimenzióból, és külön az információs dimenzióból érkező lehetséges fenyegetéseket.

A kritikus információs infrastruktúrákat az információs dimenzióból veszélyeztető – infokommunikációs – fenyegetéseket a támadó, valamint az elkövetés módja alapján csoportosítottam. **Ezek alapján arra a megállapításra jutottam, hogy a kritikus információs infrastruktúrákat az információs dimenzióból a következő tényezők veszélyeztetik:**

- a tévedő alkalmazottak;
- az elégedetlen alkalmazottak vagy szerződéses partnerek;
- a hackerek;
- a személyes előnyöket keresők;
- a szervezett bűnözés ügynökei, kereskedelmi versenytársak vagy más érdekcsoportok;
- külföldi kémszervezetek;
- terroristák;
- ellenséges fegyveres erők.

Ezen tényezők és a támadási módok elemzése alapján megállapítottam, hogy a következő – információs – támadások hajthatók végre a kritikus információs infrastruktúrák ellen:

- a szolgáltatás megtagadás jellegű támadás;
- a cracking vagy hacking, ha rendszerkárokhoz vagy a bizalmasság sérüléséhez vezet;
- a fedett vagy rosszindulatú (malware) programok, beleértve a vírusokat, férgeket, trójai programokat, hoaxokat;
- az adathalászat (phishing) bizalmas adatok megszerzésére;
- a programok hibáinak kihasználásával elkövetett betörés (botnets);
- az üzenetek jogtalan elfogása vagy lehallgatása (pl.: laptop vagy PC-k lopása, forgalom eltérítések, billentyűzet vagy hálózat lehallgatása, stb.);
- a belső munkatársak szándékos vagy gondatlan károkozása;
- az elektronikai felderítés útján az infokommunikációs rendszer adatainak megszerzése;
- az irányított energiájú fegyverekkel elkövetett támadások;
- az egyéb elektronikai támadások.

Amióta az internet mindenütt jelenlévővé vált az információs társadalmakban, a legtöbb támadás megvalósítása is áttevődött az internetre. Az internet alapú támadások sajátos jellegéből következik azok gyakorisága és hatása, azaz az internet lehetővé teszi a nagy távolságokról történő, gyakori támadásokat, ugyanakkor számos más lehetőséget is biztosít a kapcsolódott rendszerek támadására.

Esettanulmányként bemutattam a 2007 tavaszán bekövetkezett Észt-Orosz konfliktust, amely alapján azt a következtetést vonom le, hogy egy az információs dimenzióból érkező támadás komoly károkat okozhat egy fejlett infrastruktúrával rendelkező országnak. A bemutatott példa jól rávilágít arra a tényre, hogy a **védelem terén elengedhetetlenül fontos a megelőzés, a jogszabályoknak, szabványoknak, ajánlásoknak megfelelően felépített, megfelelő tartalékolással rendelkező biztonságos rendszerek kialakítása.**

Az Európai Unió és az európai országok gyakorlatát, az EU határozatait, irányelveit és javaslatait feldolgozva arra a **következtetésre jutottam**, hogy a kritikus információs infrastruktúrák védelme tekintetében **komoly előrelépések történtek**. Az egyes országok politikai vezetése megértette a problémát és **megteremtette a szükséges jogszabályi hátteret** a védelem érdekében. Az EU és a különböző országok kormányainak támogatásával a témában széles körű tudományos kutatások folynak, amelyekkel a védelmi területek,

eljárások, módszerek és megoldások tökéletesítésére törekszenek. A gazdasági szféra, mint érintett tulajdonosi kör, az állammal együttműködve részt vállal a kritikus információs infrastruktúrák védelmében. Az információs infrastruktúrák védelme tekintetében az infokommunikációs rendszerek biztonsági szabványainak bevezetésére nagy hangsúlyt fektetnek.

A nemzetközi tapasztalatok alapján **az önszerveződő, társadalmi alapokon (is) működő hálózatbiztonsági szervezetek egyre nagyobb szerepet kell, hogy kapjanak a kritikus információs infrastruktúrák védelmében**, különösen a monitorozás és az információ-megosztás (biztonságkultúra fejlesztése) területén. Ezeket a szervezeteket az egyes országokban különböző mértékben és módon támogatják, tevékenységüket összehangolják.

Kutatásaim során **megállapítottam**, hogy a **kritikus információs infrastruktúrák védelme terén az USA**, mint a legfejlettebb, az információs társadalom kiépítése terén élenjáró ország a **tette a legtöbbet** mindezidáig mind jogszabályi, mind szervezeti kérdésekben.

3. FEJEZET
A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELMÉNEK HAZAI MEGVALÓSÍTÁSA

A nemzet biztonságának megőrzése érdekében meg kell akadályozni, vagy elviselhető mértékűre kell csökkenteni a kritikus információs infrastruktúrák elleni sikeres támadások lehetőségét.

Ennek érdekében meg kell határozni az állami, önkormányzati feladatokat, az üzleti és civil szféra feladatait, valamint azok bevonásának lehetőségét az állami, önkormányzati feladatokba. Meg kell határozni, melyek az elsődleges állami feladatok, milyen erőkkel és eszközökkel végezhető a kritikus információs infrastruktúrák védelme.

Hazánk a *hagyományos* hadviselés terén politikai-gazdasági helyzetével arányos védelmi potenciált igyekszik kialakítani, és ebben szövetségi rendszerünkre a NATO-ra is támaszkodhat. A kritikus infrastruktúrák védelme, de különösen a kritikus információs infrastruktúrák védelme azonban csak részben tekinthető katonai feladatnak, mert a konkrét fenyegetés megjelenésekor már nem alakítható ki hatékony védelem és így a szövetségi rendszer sem képes megvédeni ezeket.

3.1. A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELMÉRE VONATKOZÓ RELEVÁNS HAZAI ELŐÍRÁSOK ÉS AJÁNLÁSOK

3.1.1. JOGSZABÁLYOK

A hazai kritikus információs infrastruktúrák védelmének értékeléséhez elengedhetetlen a jogi szabályozás részterületeinek átfogó vizsgálata.

A **2004. évi CV. törvény a honvédelemről és a Magyar Honvédségről** (továbbiakban: Hvt.) határozza meg a békeállapottól eltérő időszakra vonatkozó szabályokat. A honvédelmi kötelezettségek rendszere között került szabályozásra az ország területén működő jogi személy és jogi személyiséggel nem rendelkező szervezetek meghatározott gazdasági és anyagi szolgáltatásra való kötelezettsége.

A Hvt. 35.§. lehetőséget biztosít arra, hogy a honvédelmi felkészülés békeidőszakban is elrendelhető legyen, azaz a tervezetten igényelt szolgáltatás teljesítéséhez a szükséges mértékben előkészüljenek különböző szervezetek. Ez a paragrafus elvi lehetőséget biztosíthat

az elektronikus hírközlési infrastruktúrát tulajdonló és üzemeltető gazdálkodók felé a minősített időszaki szolgáltatás igénybevételi módjának szabályozására. Ez a szabályozás természetesen összhangban kell, hogy álljon a kidolgozásra tervezett nemzeti kritikus infrastruktúrák védelmi programmal.

A törvény III. fejezetében nevesítésre kerültek a honvédelemi felkészülés és egyes feladatainak ellátásában részt vevő szervek, úgymint a műsorszóró rádió- és televízióállomások, nemzeti hírügynökség, elektronikus hírközlési és az informatikai szervek. A törvény itt is egyértelműen fogalmazza meg, hogy a fenti szervek működési területükön felkészülnek a jogszabályban meghatározott honvédelmi feladataik teljesítésére, folyamatosan biztosítják a honvédelmi célú működésük feltételeit, beleértve az ehhez szükséges tervezési és előkészületi tevékenységet is. A honvédelemben közreműködő szervek feladatát – a törvény keretei között – a tevékenységi körrel érintett miniszter vagy a Kormány, rendeletben állapítja meg.

A törvény a Kormány feladatai között határozza meg, hogy gondoskodik a Honvédelmi Tanács és a Kormány speciális működésének a feltételeiről. Ebbe a megfogalmazásba értelemszerűen beletartozik a minősített időszaki irányításhoz és a vezetéshez szükséges infrastruktúra is. [4]

Látható, hogy a Hvt. igen jó alapot biztosít egy jól elkészített nemzeti kritikus infrastruktúra védelmi program – azon belül is az információs infrastruktúrák védelméhez szükséges szabályozás – törvénybe illesztéséhez.

A 2073/2004. (IV.15.) Korm. határozat a Magyar Köztársaság nemzeti biztonsági stratégiájáról foglakozik *a biztonsági környezet – fenyegetések, kockázatok, kihívások részben (II.)* az információs társadalom kihívásaival, ezen belül az informatikai és telekommunikációs hálózatok sebezhetőségével és kockázatával. *A terrorizmus elleni védekezés* részben (III. 3.1.) külön megemlíti a kritikus infrastruktúrák védelmének feladatát. Az információs rendszerek védelme részben (III. 3.7.) kiemeli a kormányzati információs rendszerek védelmének fontosságát és felhívja a figyelmet a sikeres védelem érdekében szükséges együttműködésre, az érintett informatikai és távközlési szolgáltatókkal. *„A hosszú távú lemaradás hátrányos következményeinek elkerülése érdekében Magyarország számára kiemelt feladat a felzárkózás a fejlett világ információs és telekommunikációs színvonalához. Az információs forradalom vívmányainak mind szélesebb körű megismertetése, az oktatás színvonalának emelése kulcsfontosságú érdek, ami közvetve pozitív hatással van a gazdaságra, a társadalom életére és az ország érdekérvényesítő képességére. Az informatikai infrastruktúra technikai és szellemi feltételeinek biztosítása mellett ügyelni kell e rendszerek*

védelmére és a megfelelő tartalékok képzésére is. Az informatika számtalan lehetőséget teremtett a társadalom számára, de fokozta annak veszélyeztetettségét. A számítógépes hálózatok és rendszerek sebezhetősége, túlterhelése, az információlopás, a vírusterjesztés és a dezinformáció kockázati tényezőt jelent az ország számára." [6] Ezen fenyegetésekre válaszul célul tűzi ki, hogy *„A technológia rohamos fejlődésének korában új feladatként jelentkezik a korszerű és biztonságos informatikai infrastruktúra kialakítása és a kormányzati információs rendszerek védelme. A kormányzati információs rendszert fel kell készíteni a kibernetikai támadások megelőzésére és kivédésére. A védelem sikere érdekében szoros koordináció szükséges mind a szövetségesekkel, mind az informatikai és távközlési szolgáltatók, valamint kutatóközpontok között."* [6].

A Magyar Köztársaság nemzeti biztonsági stratégiájáról szóló kormányhatározat 1. c) pontja előírja, hogy *„A Kormány ... felhívja ... az informatikai és hírközlési minisztert az informatikai és információvédelmi stratégia összehangolt, az érintett tárcák bevonásával 2005. december 31-ig történő elkészítésére azzal, hogy a stratégiák tervezetét a Nemzetbiztonsági Kabinet előzetes véleményét követően, jóváhagyásra a Kormány elé terjessze."* [6]. Ez az informatikai és információvédelmi stratégia nem került elfogadásra a mai napig[100].

A **2112/2004. (V.7.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól** 1. melléklete, a Terrorizmus Elleni Akcióterv, a kritikus infrastruktúrák védelmével összefüggő feladatokat határozott meg. E szerint fejleszteni kell a kritikus infrastruktúra biztonságának jogi alapjait és a megelőzési mechanizmusokat. Az uniós Akcióterv alapján, a kritikus infrastruktúrák védelme céljából, feladatul tűzte ki az információs rendszerek elleni támadásokról szóló kerethatározat elfogadását és egy teljesen védett, minősített adatok továbbítására is alkalmas kommunikációs rendszer kialakítását. Döntés született a felkészülésre az európai kritikus infrastruktúrák védelmére vonatkozó programhoz (EPCIP) való kapcsolódásunkra. [7]

A Terrorizmus Elleni Akcióterv felülvizsgálatáról szóló 2151/2005. (VII. 27.) Korm. határozat mellékletének (II. Akcióterv) 5. pontja célkitűzéseiben feladatot határozott meg a kritikus infrastruktúra fenyegetettségének felmérésére, elemzésére összhangban az EU

[100] Az Információs Társadalom Koordinációs Tárcaközi Bizottság Informatikai Biztonsági Albizottsága 2005. 02. 28-i ülésén ismertetésre került az elkészült informatikai és információvédelmi stratégia absztraktja [43]. Nem hivatalos források szerint ezt a változatot a Nemzetbiztonsági Kabinet nem fogadta el, ezért a GKM 2006. végén megbízást adott a Puskás Tivadar Közalapítványnak az Informatikai és Információvédelmi Stratégia áttekintésére és aktualizálására [15].

által végzett elemzéssel, és meghatározta szakértő kijelölését az EU kritikus infrastruktúra figyelmeztető hálózatába (CIWIN). [8]

A **2046/2007 (III. 19.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól szóló 2112/2004. (V.7) Korm. határozat módosításáról** 1. sz. melléklet 2.3.1. pontja előírja a Kritikus Infrastruktúrák védelem Európai Programjának megközelítését tükröző, a különböző ágazati feladat- és hatáskörbe tartozó kritikus infrastruktúrák védelmi tevékenységek közös keretrendszerbe foglalásáról, ágazatközi összehangolásáról szóló előterjesztés elkészítését. [5]

2236/2003. (X. 1.) Korm. határozat a Magyar Honvédség 2004-2013 közötti időszakra vonatkozó átalakításának és új szervezeti struktúrájának kialakításáról. A kormányhatározat 11. pontja előírja, hogy meg kell vizsgálni a védett vezetési rendszer fenntartásának szükségességét, illetve annak egyes elemei más, különösen válságkezelési célú felhasználásának lehetőségét. [9]

A katasztrófavédelemmel összefüggő 2007. évi feladatokról szóló **1/2007. (III.29.) Kormányzati Koordinációs Bizottság határozat** 5. b) pontja értelmében meg kell kezdeni a kritikus infrastruktúrák védelem nemzeti programjának kidolgozását, elő kell készíteni a kritikus infrastruktúrák védelem hazai koordinációjáról, feladatairól szóló kormány előterjesztést. [2]

Tárcaközi bizottság vizsgálta a hasznosítási lehetőségeket, és előterjesztést dolgozott ki a Kormány számára a védett vezetési rendszer létesítményeinek hasznosításról. Az előterjesztés kiemeli a rendszer egyedülálló fizikai védelmi képességeit és az ebben rejlő nemzeti értéket. Javasolja az állami hasznosítás oly módját, amely lehetőséget teremt nagyérzékenységű nemzeti adattárak és informatikai tárolók elhelyezésére. Ezzel mintegy biztosítva a NATO Prágai Nyilatkozat [90] szerinti fenyegetettségek elleni védelmi képesség kialakítását. A fenti javaslatnak megfelelően kormányhatározatok születtek a hasznosításra olyan kiegészítéssel, hogy meg kell vizsgálni annak a lehetőségét is, hogy az üzleti élet résztvevőire kiterjeszthető legyen a fenti célú hasznosítás (természetesen a biztonsági szabályok betartásával). A hasznosítás koordinálására a honvédelmi miniszter jogosult.

A kilencvenes évek közepén kormányhatározat született a fontosabb objektumok minősített időszaki őrzéséről és azok védelmének besorolási elveiről. Ez alapján jegyzékek készültek a honvédelmi érdekből fokozott védelmet igénylő objektumokról. A jegyzékek frissítése alkalmat teremthet a kritikus információs infrastruktúrák védelmének uniós szempontrendszer szerinti harmonizációjára.

További jogszabályok, amelyeket a kritikus információs infrastruktúrák védelmének kialakításakor figyelembe kell venni:

Az államtitok és a szolgálati titok védelme, rejtjeltevékenység:

- Az **1995. évi LXV. törvény az államtitokról és a szolgálati titokról** 30. § (2) bekezdése előírja, hogy *„A Kormány az érintett állami szervek vezetőivel egyetértésben a minősített adatot kezelő információs rendszerek létesítésének és működésének rendjét 1995. december 31-ig határozza meg."* [3] Ugyanakkor megállapítható, hogy ez a mai napig nem történt meg! A törvény módosítása évek óta napirenden van, különböző változatait készítették már el, de még nem került az Országgyűlés elé.
- 43/1994. (III, 29.) korm. rendelet a rejtjeltevékenységről;
- 2000. évi IV. tv. az információ biztonságáról szóló Brüsszelben 1997. március 6-án kelt NATO megállapodás megerősítéséről és kihirdetéséről;
- 1998. évi LXXXV. tv. a Nemzeti Biztonsági Felügyeletről;
- 180/2003. (XI. 5.) korm. rendelet a Nemzeti Biztonsági Felügyelet részletes feladatairól és működési rendjéről, valamint az iparbiztonsági ellenőrzések részletes szabályairól;
- A nemzetbiztonsági szolgálatokról 1995. évi CXXV. törvény.

Elektronikus aláírás:

- 2001. évi XXXV. tv. az elektronikus aláírásról;
- 194/2005. (IX. 22.) korm. rendelet a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokkal kibocsátó hitelesítésszolgáltatókra vonatkozó követelményekről;
- 15/2001. (VIII. 27.) MeHVM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról;
- 16/2001. (IX.1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről;
- 2/2002. (IV.26.) MeHVM irányelv a minősített elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről;
- 2003. évi C. törvény. az elektronikus hírközlésről.

Elektronikus információvédelem honvédelmi szerveknél:

- 33/2002. (HK 13.) HM utasítás az elektronikus információvédelemről.

Információs társadalom:

- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

3.1.2. AJÁNLÁSOK

A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága ajánlásai

A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) *Informatikai biztonsági módszertani kézikönyv* címet viselő, 1994-ben kiadott MeH ITB 8. számú ajánlása a brit kormány Központi Számítógép és Távközlési Ügynökség (Central Computer and Telecommunications Agency) *CCTA Risk Analysis and Management Method* és az északrajna-vesztfáliai kormány *Informationtechnik Sicherheitshandbuch* felhasználásával, valamint az EU informatikai ajánlásai és a hazai jogszabályok alapján készült. A kézikönyv célja a szervezetet az informatikai biztonsági koncepciójának kialakítására történő felkészítés volt. A biztonsággal kapcsolatos legfontosabb tudnivalók, valamint az informatikai biztonság és a szervezet összbiztonsága közötti összefüggések meghatározó elemei a kézikönyvhöz csatolt mellékletekben találhatók meg. A MeH ITB 8. számú ajánlását, mint az informatikai biztonság – CRAMM alapú – kockázatelemzési módszertanát a közigazgatás területén kívül is elterjedten használják. [83]

A MeH ITB kezdeményezésére 1995-ben kezdődött meg a következő hazai ajánlás kidolgozása, amelyet 1996 decemberére véglegesítettek, és az *Informatikai Rendszerek Biztonsági Követelményei* címmel, mint a *MeH ITB 12. sz. ajánlás* vált nem hivatalos szabvánnyá. Az *Informatikai Rendszerek Biztonsági Követelményei* kidolgozásánál elsődleges szempont volt, hogy ne csak a logikai védelem előírásait tartalmazza, hanem jelenjenek meg benne az adminisztratív és a fizikai védelem követelményei is. A logikai védelem (hardver, szoftver, hálózatok) esetében az ITSEC került adaptálásra, ugyanakkor részletes követelményeket és védelmi intézkedéseket tartalmaz az informatikai biztonság adminisztratív és a fizikai védelem területeire, a szervezeti, személyi és fizikai biztonság kérdéseire is. A gazdasági élet számos szereplője a saját biztonsági politikája kialakításakor figyelembe vette a 12. sz. ajánlást, több esetben a mai napig is belső szabályzóként, követelményrendszerként használják a biztonsági követelmények meghatározására. Mivel ma már az ITSEC dokumentumot nem használják, így a 12. számú ajánlás is elavulttá vált. [82]

Az CC feldolgozására és honosítására irányuló munka hazánkban 1997-ben kezdődött, majd 1998-ban a MeH ITB 16. sz. ajánlásaként *Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertana* címen, mint a Common Criteria 1.0 változatának hazai feldolgozása kiadásra került.

Magyar Információs Társadalom Stratégia – Informatikai Biztonsági Részstratégia

2002 végén a kormány elfogadta az Informatikai és Hírközlési Minisztérium által készített *Magyar Információs Társadalom Stratégiát*, majd 2003-ban elkészült ennek *Informatikai Biztonsági Részstratégiája*.

Informatikai Biztonsági Részstratégia I. kötete részletes kitekintést ad az informatikai biztonság nemzetközi helyzetére. A II. kötet stratégiai célokat és feladatokat szab meg a biztonságos információs társadalom érdekében. Ezek között már szerepel a kritikus információs infrastruktúrák védelme is! [85]

A nagyon jó stratégiai munkaanyag felhasználása lendületesen elkezdődött, majd az Informatikai és Hírközlési Minisztérium megszűnésével gyakorlatilag a stratégia és annak biztonsági részstratégiája is a feledés homályába merült a kormányzat részéről.

Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma

Az informatikai biztonság munkáinak hatékonyabb végrehajtása érdekében szükség volt a nemzeti, a NATO és az EU követelmények és feladatok egységes szakmai szempontokra épülő kezelésére. Ennek keretében indult meg a jelenlegi helyzetet figyelembe vevő jogszabályi szintű elektronikus információvédelmi szabályok kialakítása, és kezdődtek el a szabályok érvényesülését lehetővé tevő szervezeti struktúraváltoztatásokkal kapcsolatos tervek kidolgozása, és elkezdődtek a szervezetek egymás közötti, és az informatikai biztonságba vetett bizalmat erősítő tudatosítási és képzési munkálatok.

A Magyar Információs Társadalom Stratégia készítéséről rendelkező 1214/2002. (XII.28.) sz. Kormányhatározat többek között az alábbi feladatot tűzi ki: *„Ki kell alakítani az informatikai alkalmazások minőségének és biztonságának hiteles tanúsítási rendjét, az ehhez szükséges jogszabályok megalkotásával és intézményrendszer felállításával."*

A kormányhatározat végrehajtásával párhuzamosan hazánk csatlakozott a Common Criteria (CC, Közös szempontok, MSZ ISO/IEC 15408) egyezményhez. Csatlakozásunkkal kapcsolatosan elkezdődött egy saját nemzeti séma, a *Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)* felállítása, melynek során ki kell alakítani a megfelelő bevizsgálási, auditálási folyamatokat az informatikai eszközök biztonságának ellenőrzésére.

Részben a CC egyezményhez való teljes csatlakozás támogatására, a hazai hiteles tanúsítási rendszer kialakítását elősegítendő, részben a nem nemzetközi alkalmazásra szánt informatikai termékek biztonsági bevizsgálását elősegítendő készült el a Common Critéria-n

alapuló, a *Common Evaluation Methodology for Information Technology for Information Technology Security* egyszerűsített (honosított) változataként a MIBÉTS.

A MIBÉTS az új informatikai rendszerek bevezetése, a működő rendszerek – az informatikai sajátosságokból adódó – folyamatos megújítása, fejlesztése során, a tervezéstől a bevezetésig figyelembe veendő technológiai biztonsági szempontok kialakításához és értékeléséhez nyújt támogatást. A MIBÉTS dokumentumok az informatikai rendszer kialakításáért felelős vezetők, szakemberek (informatikai termékfejlesztők, rendszer-integrátorok), továbbá a technológia szempontú értékelést és tanúsítást végzőknek szól. [85]

Magyar Informatikai Biztonság Irányítási Keretrendszer

Újra utalva a Magyar Információs Társadalom Stratégia készítéséről rendelkező 1214/2002. (XII.28.) sz. Kormányhatározat 4.2. pontjára, az Informatikai és Hírközlési Minisztérium 2004-ben úgy döntött, hogy a nemzetközi trendekkel összhangban kidolgoztatja a szervezeti szintű informatikai biztonság követelményeit és a vizsgálat rendjét, mint az Információs Társadalom Koordinációs Tárcaközi Bizottság ajánlásait. Ehhez figyelembe kívánták venni az ISO/IEC 17799 nemzetközi szabványt, az ISO/IEC TR 13335 szabványt, továbbá a NATO (Security within the North Atlantic Treaty Organisation (NATO) – C-M(2002)49) és az Európai Unió (Európai Unió Tanácsának Biztonsági Szabályzata (2001/264/EK) releváns szabályozásait. [85]

A szervezeti szintű informatikai biztonsági ajánlástervezetek közös, összefoglaló elnevezése a *Magyar Informatikai Biztonság Irányítási Keretrendszer* (MIBIK). A MIBIK – jelenleg – két kötetből áll. Az első *Az Informatikai Biztonság Irányításának Követelményrendszere (IBIK)* [37], a második *Az Informatikai Biztonság Irányításának Vizsgálata (Tanúsítása) – módszertan (IBIV)* [38] címet viseli.

A releváns nemzetközi és hazai előírások és ajánlások áttekintése és összehasonlítása során **jelentős hazai lemaradásokat állapítottam meg**.

A kritikus információs infrastruktúrák védelméhez kapcsolódó területeken Magyarországon rendkívül nagy a lemaradás. **Ez a szakterület elhanyagoltságát mutatja!** A különböző jogszabályok ellentmondásai a felelősség megosztásához, elhárításához nagymértékben hozzájárulnak. Az információs infrastruktúrák és infokommunikációs rendszerek védelmére irányuló aktuális hazai előírások, ajánlások hiányosak, sőt sok esetben teljesen hiányoznak. A magyar Zöld Könyv a kritikus infrastruktúrák védelméről társadalmi, szakmai egyeztetés nélkül – információim szerint – elkészült, de még nem került publikálásra.

Tekintettel arra, hogy a kritikus infrastruktúrák védelmének biztosítása egyaránt állami és üzemeltetői érdek, ezért úgy gondolom, hogy fel kell készülni az európai uniós források felhasználására, és meg kell teremteni a védelmi intézkedések finanszírozásának új konstrukcióját, a PPP kialakítását, a magánszféra bevonását. Az Európai Unió pályázati rendszerében ezen a téren Magyarország – mint sok más esetben is – nem képviselteti magát, ami költségvetési szempontból szintén igen fontos lenne.

3.2. A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELMÉNEK HAZAI GYAKORLATA

A hazai helyzet fonákságát jelzi, hogy az Informatikai Vállalkozások Szövetsége (IVSZ) *Kritikus infrastruktúrák védelme – társadalmi feladat vagy üzleti lehetőség?* címmel honlapján 2007 augusztusában az alábbi nyilatkozatot tette közé:

„'*Az információs hadviselés a hadviselés egy új formája, amikor is az információ, illetve támadások az információ, illetve az információs rendszerek ellen a hadviselés eszközeivé válnak.' Az állami szerepvállalás a védelemre kell összpontosuljon, és e védelem kapcsán a gazdaság működőképességének fenntartása, a társadalom, a kultúra fenntartása és fejlődési ütemének biztosítása fogalmazhatók meg fő célokként. Éppen ezért az IVSZ támogatja egy olyan állami intézmény kijelölését, vagy létrehozását, amely egyszemélyben felelős az információs hadviseléshez kötődő, különösen a kritikus információs infrastruktúrák védelmével kapcsolatos feladatok meghatározásáért, koordinálásáért, végrehajtásáért, ellenőrzéséért. Az IVSZ felajánlja szakmai segítségét a fenti intézménynek a megfelelő jogszabályok előkészítéséhez, illetve szakmai szervezetként részt kíván venni a jogszabálytervezetek, előterjesztések véleményezésében. Az IVSZ szeretné, ha a tagszervezetei részt vennének a fentiek szerint megfogalmazott feladatok és projektek végrehajtásában. Jelen információink szerint a kritikus infrastruktúrák védelmének kutatási feladataira az EU az FP7 program keretében 40 millió Euró-t különített el (ICT-SEC-2007.1.7).*" [13]

A **fentiek egyértelműen jelzik**, hogy hazánkban az üzleti szféra résztvevői a kormányt megelőzve felismerték, hogy összehangolt lépeseket kell tenni a Magyar Köztársaság kritikus információs infrastruktúrájának védelme érdekében.

3.2.1. A KORMÁNYZATI ÉS KÖZIGAZGATÁSI FELADATOK TELJESÜLÉSE, A VÉDELMI IGAZGATÁS SZEREPE

A kritikus infrastruktúrák védelme feladatainak kapcsán a Magyar Tudományos Akadémia számára készített tanulmányában Dr. Botz László a következő álláspontot képviselte: *„Az Európai Unió által elindított Kritikus Infrastruktúrák védelme ... programban megfogalmazott elvárások országos, az egész társadalmat érintő feladatokat érintenek, amelyek egységes értelmezése, koordinálása, a teljesítéshez szükséges feltételek biztosítása kormányzati felelősség. (És mivel a Magyar Köztársaság – az EU teljes jogú tagjaként – vállalta a programban való részvételt, a végrehajtás integrációs (kül) politikánk szerves részét képezi.)”* [24]

Ez a **megállapítás is alátámasztja azt a következtetésemet**, hogy ezen a területen **elődleges a kormányzati felelősség**. A szükséges állami feltételek biztosítása nélkül a kritikus infrastruktúrák védelmében szerepet játszókkal szemben érdemi elvárások nem fogalmazhatók meg.

A központi, politikai, kormányzati feladatok elemzése és értékelése során **arra a megállapításra jutottam**, hogy általában az olyan védelmi feladatok, amelyek nem kötődnek közvetlenül a szövetségi rendszereinkhez, a NATO-hoz, vagy az Európai Unióhoz, **számtalan hiányosságot mutatnak**. Megállapítható, hogy elsősorban az érzékelhető külső kényszer, például a terrorizmus elleni elvárt fellépés hatására jelennek meg kormányzati intézkedések. Olyan területeken, mint kritikus infrastruktúrák védelme, az információvédelem, az infokommunikációs rendszerek biztonsága többnyire csak a hangzatos politikák, stratégiák szintjén maradnak az intézkedések.

Az is megállapítható, hogy az e téren tapasztalható elmaradásunk egyre nő, és ezt egyre nehezebb lesz bepótolni, másrészt a hiányosságok gyengeséget is jelentenek, és ez egy potenciális támadóban kihívást generálhat.

A magyar védelmi igazgatás szereplői aktív részt vállaltak a 2005. évi, az Európai Bizottság által kiadott EPCIP Zöld Könyvnek a véleményezésében, valamint annak az informatikai és elektronikus hírközlési szolgáltatókkal történő egyeztetésében. Az EPCIP kialakításával, valamint végrehajtásával kapcsolatos tevékenység elsősorban a beérkező anyagok véleményezését, az érintett szervezetekkel történő kapcsolattartást, a vonatkozó jogszabályi környezet kialakításában történő részvételt, valamint a hazai és az eseti jelleggel

külföldön történő konzultációkon/konferenciákon történő részvételt és szakértői tevékenységet foglalja magában.

A nemzetközi igényekkel párhuzamosan, nemzetközi tapasztalatokra alapozva szakmai elemzések készültek, illetve készülnek az infokommunikációs infrastruktúra létfontosságú elemei védelmének hazai és nemzetközi szabályozásáról, a lehetséges veszélyforrások azonosításáról, sérülések hatásainak elemzéséről. Összefoglaló elemzések és javaslatok kerültek kidolgozásra a kritikus infrastruktúra lehetséges definícióiról, a létfontosságú elemek meghatározására, a veszély, kockázat és sebezhetőség értékelésére alkalmas vizsgálati módszerekről, valamint a nemzeti és ágazati ütemterv megvalósításáról.

A NATO Válságreagálási Rendszerhez (NCRS) illeszkedő hazai intézkedési tervek kidolgozása, valamint a kritikus infrastruktúrák védelmével kapcsolatos többszintű biztonsági intézkedési rendszer kialakításához szükséges ágazati feladatok előkészítése érdekében készültek ezen védelmi tervek, amelyek elemzése folyamatban van.

A kritikus információs infrastruktúrák védelemével kapcsolatban felmerül az informatikai és hálózati biztonsággal kapcsolatos nemzetközi képviselet feladatainak ellátása, az ENISA munkájának nemzeti vonatkozásainak koordinációja, a kormányzati hálózati incidenskezelő központ feltételeinek biztosítása, valamint a kritikus infrastruktúra-védelmi rendszerekhez való kapcsolódás biztosítása (CERT-Hungary Központ). A kormányzati kezdeményezések keretében az informatikai és elektronikus hírközlési terület vonatkozásában nemzeti kapcsolattartó pont is kijelölésre került.

A megfelelő szintű infokommunikációs biztonság csak úgy teremthető meg, ha az társadalmi méretekben egyenszilárdságú. Ennek elérése érdekében szakmailag felkészült támogató csoportok – CERT-ek vagy CSIRT-ek – kialakítását, és működtetését végzi a Miniszterelnöki Hivatal, a felügyelete alatt álló Puskás Tivadar Közalapítvány közreműködésével. Ebben a tekintetben kiemelt feladatként jelentkezik a CERT tevékenység és a katasztrófavédelem összehangolása, valamint a specifikus K+F feladatok végrehajtása.

E feladatokat a CERT-Hungary Központ látja el. A CERT-Hungary Központ, mint közreműködő szervezet látja el az Országos Informatikai és Hírközlési Főügyelet ügyeleti feladatait[101]. A Főügyeleti rendszerben megtalálhatók a jelentősebb elektronikus hírközlési szolgáltatók, amely révén naprakész, valós idejű információk állnak a hálózatüzemeltetők és informatikai szolgáltatók rendelkezésére. Ez azt jelenti, hogy a kritikus infrastruktúra

[101] A 27/2004. (X.6.) számú IHM rendelet 19/2005. (XII.27.) számú módosítása alapján.

elemeket üzemeltető elektronikus hírközlési szolgáltatók számára egy olyan fórumrendszer, és értesítési, riasztási hálózat áll rendelkezésre, amelyből a kritikus infrastruktúra bármely okból történő sérüléséről haladéktalanul értesülnek.

A CERT-Hungary nemzetközi téren is aktívan közreműködik a kormányzati hálózatbiztonsági központok munkájában: 2007. február 2. hatállyal a Központot felvették az Európai Kormányzati CERT-ek Csoportjába (EGC), továbbá teljes jogú tagja a Magyarország mellett a legfejlettebb államok kormányzati szerveit tömörítő International Watch and Warning szervezetnek. A CERT Hungary Központ nemzetközi elismertségét jelzi, hogy megkapta a hálózatbiztonsági központok világszervezetének (Forum of Inciden Response Teams) és európai szervezetének (TF-CSIRT) akkreditációját (Trusted Introducer) is.

A CERT Hungary Központ kormányzati jellegének köszönhetően egyben nemzeti koordinációs pontként is működik, mely tevékenység keretét a hálózatbiztonság terén működő vagy ahhoz kapcsolódó civil, kormányzati és üzleti szervezetekkel kötött együttműködési megállapodások szabják meg. Ilyen szerződések kerültek aláírásra a következő felekkel: Nemzeti Nyomozóiroda, BME Vírus Kompetencia Központ, eSec.hu konzorcium, MTA SZTAKI, HUN-CERT, ISACA Információrendszer Ellenőrök Egyesülete, Magyar Nemzeti Bank, Magyar Tartalomipari Szövetség, Infomediátor, valamint egyes kereskedelmi bankokkal.

A CERT Hungary Központ közfeladatként az informatikai és hálózati biztonsággal kapcsolatos tudatosság növelését is felvállalta mind az egyéni felhasználók [11], mind a szakemberek [12] számára.

Jelenleg a következő területek vizsgálata folyik az informatika és elektronikus hírközlés kritikus vonatkozásainak területén:

- a kritikus infrastruktúra és a kritikus információs infrastruktúra fogalmi meghatározása;
- a kritikus információs infrastruktúrát fenyegető veszélyek felmérése;
- az infokommunikációs kritikus infrastruktúra elemekre vonatkozó adatok körének és információinak összegyűjtési módjainak vizsgálata az NHH bevonásával;
- a magyarországi infokommunikációs biztonság helyzet-, és kockázatelemzése (elsősorban a CERT- HUNGARY központ bevonásával);
- az EU kritikus infrastruktúrák védelem európai programból (EPCIP) és az Európai Bizottság által kiadott Zöld Könyvből fakadó feladatok elemzése;
- aktív kapcsolattartás az Európai Bizottság INFSO főigazgatóságával.

Véleményem szerint a magyar közigazgatás **szakmailag kész és képes** az Európai Unió valamint a NATO elvárásaival, ajánlásaival összhangban a Magyar Köztársaság **kritikus információs infrastruktúráinak védelmi kérdéseit megoldani**. **Ehhez azonban hiányzik az egyértelmű és következetes állami-politikai akarat, és így a támogatás is.**

Mint már korábban megállapítottam az önszerveződő, társadalmi alapokon (is) működő hálózatbiztonsági szervezetek egyre nagyobb szerepet kapnak a kritikus információs infrastruktúrák védelmében. **Megítélésem szerint a CERT-ek ezt a tevékenységet valóban képesek jól ellátni**, különösen a monitorozás és az információ-megosztás (biztonságkultúra fejlesztése) területén. A CERT-HUNGARY a nehéz, sokszor visszás hazai viszonyok között is jól teljesít, és ezt ki kell használni a kritikus információs infrastruktúra védelme során.

3.3. JAVASOLT FELADATOK A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELMÉHEZ

Kutatásaim során megállapítottam, hogy az utóbbi másfél-két évtized változásai, a globalizáció, a privatizáció és a liberalizáció **jelentős mértékben változtatta meg az információs infrastruktúra biztonsági kockázatait**. A piaci erőfölénnyel szembeni verseny újabb kockázatvállalásokat követelt, főként a kisebb szolgáltatóktól, ami tovább gyengítette a szolgáltatások biztonságát.

Ugyanakkor a technológiában lezajlott generációváltás jótékony hatással volt a megbízhatóságra, azonban ez a kompenzáció nem teljes.

A jogrendszer a piac változásait csak követte, amely azt eredményezte, hogy átmenetileg joghézagok keletkeztek. Az állam egykori gondoskodó szerepének hiánya új eszközöket, új megoldásokat, egyben drámai takarékosságot kényszerített ki a piaci szereplőkből. E folyamat kedvezőtlen hatást gyakorolt a szolgáltatók közötti – korábban zavartalan – együttműködésre, végső soron a szolgáltatás megbízhatóágára, a szolgáltatók túlélő képességére.

Az infokommunikációs infrastruktúrák ma számottevő különbséget mutatnak mind technológiájukban, mind rendeltetésükben. Így a legkisebb személyi számítógéptől a nagy kiterjedésű antennarendszerekkel rendelkező rádióadókig a legkülönbféle problémával és kockázati tényezővel kell számolni. Külön kell vizsgálni az egymással függőségi viszonyban lévő infrastruktúrákat, azoknak az infokommunikációs rendszerekre, hálózatokra gyakorolt hatását, kockázatait (pl.: a villamosenergia-ellátás hatása az infokommunikációra).

3.3.1. JAVASOLT KORMÁNYZATI ÉS KÖZIGAZGATÁSI INTÉZKEDÉSEK

A piaci feltételek között megvalósuló működés, a biztonságkultúra és a biztonságtudatosság jelenlegi színvonala nem ad megfelelő garanciákat a kritikus információs infrastruktúrák megfelelő védelmére, ezáltal hazánk működőképességének fenntartására, túlélőképessége szükséges szintjének elérésére és fenntartására. A kritikus információs infrastruktúra bármely elemének jelentősebb kiesése az országban különböző mértékben zavart, működésképtelenséget okozna. A minősített időszak előírásaival foglalkozó jogszabályok e kérdéskört elkerülik.

Mindezek alapján a védelmi képességek megteremtése érdekében javaslom:

- **Egy nemzeti kritikus infrastruktúra védelmi program létrehozását** a kritikus infrastruktúra üzemeltetők, a kutatóintézetek, valamint az állami szféra minél szélesebb körben történő tájékoztatására és pályázati hajlandóságuk elősegítésére, különös tekintettel a jelenlegi költségvetési lehetőségekre, amelyek a kritikus infrastruktúrák védelmi programjainak teljes körű finanszírozását nem teszi lehetővé. Tekintettel arra, hogy a létfontosságú infrastruktúrák védelmének biztosítása egyaránt állami és üzemeltetői érdek, meg kell teremteni a védelmi intézkedések finanszírozásának új, PPP konstrukciójú kialakítását. Fel kell készülni az EU források felhasználására is, amely ugyancsak nagymértékben igényli a magánszféra bevonását.
- **A kritikus infrastruktúrák védelmi követelményeit külön – parlamenti konszenzuson alapuló – törvényben, valamint alacsonyabb szintű jogszabályokban rögzíteni**, mert csak így oldható meg, hogy parlamenti, kormányzati ciklusokon keresztül is a célok érvényesíthetők legyenek, anélkül, hogy napi politikai viták tárgya lenne.
- **A kritikus infrastruktúrák védelmében érintett kormányzati, gazdasági és társadalmi szereplők között a politikai és stratégiai célok tekintetében konszenzust teremteni**, és e konszenzuson, valamint **jogszabályi alapokon nyugvó koordinációt létrehozni.** A konszenzus segít abban, hogy a védelmi feladatokat a gazdasági és társadalmi szereplők is magukénak érezzék a kritikus infrastruktúrák védelmét, közmegegyezésen nyugvónak tartsák, ahol az irányítás kérdéseibe beleszólásuk van, ugyanakkor a jogszabályi keretek biztosítják, hogy az állam a védelmi feladatok területén megfelelő jogi háttérrel is rendelkezzen.

- Az állami közfeladatok fontosságának megfelelően **fejleszteni** a polgári-, a katonai- és a rendvédelmi szervek közötti együttműködést, különös tekintettel a katasztrófavédelmi szervekre.
- **Fokozni** a terrorelhárításban érdekelt szervek és a terrorveszélyeztetett szervezetek-szolgáltatók közös tervezési és felkészítési munkáját.
- Az állami-, az ágazati- és vállalati tartalékolás **összehangolását**, a finanszírozás feltételeinek **szabályozását.**
- Állami szabályozókkal **megteremteni** a gazdálkodó szervezetek és személyek számára a (piaci) feltételeket a kritikus infrastruktúrák védelmével összefüggő közfeladatok végzéséhez.
- **Alkalmazni** az EU szakmai szervezeteinek és a NATO polgári szervezeteinek (CCPC) ajánlásait és dokumentumait a hazai védelmi tervezésben, beleértve a minősített iratkezelés hazai szabályozását is.
- Az infokommunikációs rendszerek biztonságával kapcsolatos ajánlásokat, módszertani segédanyagokat **kiadni.**
- Jogszabályi keretek között, államilag elismert vizsgáló laboratóriumokkal **elvégeztetni** az eszközök és létesítmények biztonsági osztályba sorolását, értékelni a védelmi megoldásokat.
- A biztonsági auditot, kockázatelemzést, termék vagy rendszertanúsítást végző cégek kijelölésében, ellenőrzésében az államnak nagyobb **szerepvállalását.**
- Az élőerős őrzés minősített időszaki többlet igényét kiszolgáló struktúra kialakítását.
- Megfelelő, államilag támogatott **monitoring rendszer kialakítását**. E feladatokat a CERT-Hungary Központ látja el, amelynek a Nemzeti Kritikus Infrastruktúra kezdeményezések során meghatározó szerepet kell kapnia, mind a kormányzati, mind a kritikus infrastruktúra üzemeltetőinek infokommunikációs biztonsági feltételeinek megteremtése és javítása során.

3.3.2. JAVASLAT A MAGYAR KÖZTÁRSASÁG INFOKOMMUNIKÁCIÓS BIZTONSÁGI STRATÉGIÁJÁRA

A kritikus információs infrastruktúrák védelmi feladatai jelentős tervező munkát, gondos előkészítést igényelnek. A központi és ágazati szabályozás, az irányító, koordinációs testületek munkába állása is jelentős időt vesz igénybe. A korábbi években végzett tanácsadó tevékenységem során azt tapasztaltam, hogy a kormány által kiadott biztonsági

dokumentumokat, stratégiákat, kormányzati ajánlásokat a gazdasági és civil szféra akkor is felhasználja, ha az nem kötelező.[102] A kritikus információs infrastruktúrák védelmi kérdésében az egyik legfontosabb iránymutatás az *infokommunikációs biztonsági stratégia*, hiszen a kritikus információs infrastruktúrák meghatározó mértékben infokommunikációs rendszerekből állnak, vagy azok szolgáltatásira épülnek.

A fentiek alapján elkészítettem és javaslatot teszek a hazai infokommunikációs biztonsági ágazati stratégia-tervezetre, amely tartalmazza a nemzeti célokat és feladatokat ezen a téren.

Az infokommunikációs biztonsági stratégiát a **Magyar Köztársaság nemzeti biztonsági stratégiájára** (2073/2004. (IV. 15.) Korm. határozat) **épülve**, azzal **összehangolt ágazati stratégiaként készítettem el.**

A kidolgozás során figyelembe vettem a kutatásaim során levont következtetéseket, valamint a 2073/2004. (IV. 15.) Korm. határozat 1. c) pontjában meghatározottakat, azaz az infokommunikációs technológiai alkalmazások széles társadalmi elterjedtségét, és az infokommunikációs eszközöket kihasználó, illetve ezek ellen irányuló fenyegetettségeket.

A nemzeti biztonsági stratégia II.1.6. (az információs társadalom kihívásai) és a III.3.7. (információs rendszerek védelme) pontjait figyelembe véve, az infokommunikációs biztonsági stratégia védendő értékként azonosítottam az ország működése szempontjából létfontosságú infokommunikációs rendszereket, az úgynevezett kritikus információs infrastruktúrákat és azok felhasználóit, valamint védendő érdekként határoztam meg az ilyen rendszereken kezelt adatok bizalmasságát, sértetlenségét, és rendelkezésre állását.

A stratégiában elemzem a hazai és nemzetközi biztonsági környezetet, a kockázatokat, fenyegetéseket és kihívásokat.

A stratégia általános célkitűzése a nemzet biztonságának megőrzése azáltal, hogy megakadályozza, vagy elviselhető mértékűre csökkenti a kritikus információs infrastruktúrák elleni sikeres támadások lehetőségét, valamint a bekövetkezett támadások hatását a lehető legkisebbre csökkentse. Ennek érdekében a következő célokat tűzi ki:

- a kritikus információs infrastruktúrák elleni támadások hatékony megelőzése;

[102] A legmarkánsabb példa a MeH ITB 12. sz. ajánlása, amelyet a közigazgatás számára bocsátottak ki. A közigazgatásban – anyagi okokra hivatkozva – gyakorlatilag sehol sem vezették be. A közigazgatáson kívüli nagyvállalati szféra (például: MATÁV Rt., Paksi Atomerőmű Rt., TITÁSZ Rt., Dunaferr Rt.) a kiadást követő két éven belül belső szabályzóként bevezette, és használatba vette.

- a kritikus információs infrastruktúrák elleni támadások hatékony kivédése;
- a kritikus információs infrastruktúrák elleni támadások hatékony kezelése.

A célok megvalósításához szükséges feladatok terén a stratégia meghatározza az állami koordináció szükségességét, valamint a már meglévő eredményekre épülő monitorozás és reagálás elmélyítését. További feladat az informatikai biztonsági jogszabályok, szabványok, ajánlások aktualizálása, illetve megteremtése, valamint az infokommunikációs rendszerekbe vetett bizalom erősítése a biztonságtudatosság és az ismeretek fejlesztésén keresztül. Kiemelendő, hogy a feladatok végrehajtása az üzleti, civil és akadémia szféra széleskörű bevonását, valamint a nemzetközi szövetségesi rendszer használatát, illetve fejlesztését igényli.

Az infokommunikációs biztonsági stratégia egyben kapcsolódik a NATO és az Európai Unió információbiztonsággal, infokommunikációs biztonsággal kapcsolatos elvárásaihoz és törekvéseihez, továbbá a nemzetközi tapasztalatokra építve figyelembe veszi a hazai közigazgatási, gazdasági és társadalmi környezetet és azok elvárásait.

3.3.2.1. A MAGYAR KÖZTÁRSASÁG INFOKOMMUNIKÁCIÓS BIZTONSÁGI STRATÉGIÁJA

I. Értékek és érdekek

Magyarország sikere a globalizálódó világban jelentős mértékben múlhat az információs társadalomba való átmenet hatékonyságán: az egyének és szervezetek birtokában lévő információ ugyanis létfontosságú erőforrás. Mind az információ, mind az ahhoz tartozó folyamatok, rendszerek és eszközök egyre jelentősebb értéket képviselnek, olyan kiemelt jelentőségű erőforrásokká váltak, amelyek semmi mással nem helyettesíthetők. Így megnövekedett a kormányzati szektor és a gazdálkodó szervezetek működőképességének az infokommunkiációs rendszerektől való függősége, és új típusú kockázatok jelentek meg, melyek hatékony kezelése nélkül az információs társadalom nem fejlődhet.

A különféle szervezetek hatékony vezetése és rendeltetés szerinti működtetése csak a szükséges információ birtokában valósítható meg. Ha az információ nem férhető hozzá, elvész vagy illetéktelen kezekbe jut, az jelentős anyagi és erkölcsi károkat okozhat, ezért védeni kell.

Ennek megfelelően az „informatikai biztonság” ma már „infokommunikációs biztonság”, ami nem csak a számítástechnikára, hanem egy szerteágazó területre vonatkozik.

Az infokommunikációs rendszerek magukba foglalják az adatok gyűjtésére, felvételére, tárolására, feldolgozására (megváltoztatására, átalakítására, összegzésére, elemzésére, stb.), továbbítására, törlésére, hasznosítására (ideértve például a nyilvánosságra hozatalt is), és felhasználásuk megakadályozására használt elektronikus eszközöket, eljárásokat, valamint az üzemeltető és a felhasználó személyeket is. Az infokommunikációs rendszerekhez tartoznak:

- az informatikai rendszerek és hálózatok, ide értve az internet szolgáltatást is;
- a vezetékes, a mobil, a rádiós és műholdas távközlés;
- a vezetékes, a rádiófrekvenciás és műholdas műsorszórás;
- a rádiós vagy műholdas navigáció;
- az automatizálási, vezérlési és ellenőrzési rendszerek (SCADA, távmérő, távérzékelő és telemetriai rendszerek, stb.);
- a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek eszközei, eljárásai, valamint az üzemeltető és a felhasználó személyek is.

I.1. A védelem alanyai és tárgyai

Az infokommunikációs rendszereket már ma is számos célra használjuk, és az információs társadalom továbbfejlődésével folyamatosan bővül azoknak a tevékenységeknek a köre, melyeket elektronikusan lehet majd végezni. Már most is elmondható, hogy a felhasználók infokommunikációs rendszert használhatnak:

- hatósági és intézményi ügyintézésre (központi vagy helyi szinten);
- gazdasági tevékenységek támogatására;
- gazdasági kapcsolatra;
- a gazdálkodó, továbbá az állami és közigazgatási szervezeten belüli irányításra, ellenőrzésre és (vagy)
- magáncélra.

Mindez azt is meghatározza, hogy kik használnak infokommunikációs rendszert, tehát kikre terjed majd ki az infokommunikációs biztonsági szabályozás alanyi hatálya, mint felhasználókra (a továbbiakban együtt: felhasználó):

(a) a központi vagy helyi állami és közigazgatási szervezetre:
- egyfelől, mint elektronikusan ügyet intéző hatóságra, mint más szervezettel információt cserélő alanyra, mint állam- vagy szolgálati titkok kezelőjére, mint személyes adatok és bizalmas adatok (üzleti és magántitok) kezelőjére, mint elektronikusan szerződést kötő félre, mint információs társadalommal összefüggő szolgáltatások, illetve távközlési szolgáltatások igénybevevőjére, mint

infokommunikációs rendszert használók munkáltatójára, esetleg, mint – az informatikai biztonsággal kapcsolatos bűncselekménnyel – érintettre;

– másfelől az egyes állami és közigazgatási szervezetekre, mint az informatikai biztonság és az ezzel összefüggő szakterületek (pl. infokommunikációs rendszerek vizsgálata, minősített adatok kezelése stb.) szabályozásáért, koordinálásáért, érvényesítéséért, ellenőrzéséért felelős, vagy ebben közreműködni köteles szervezetekre;

(b) a gazdálkodó szervezetre, mint közigazgatási ügyfélre, elektronikusan szerződést kötő és a gazdasági életben résztvevő félre, információs társadalommal összefüggő szolgáltatások, illetve távközlési szolgáltatások igénybevevőjére, mint a személyes adat kezelőjére, mint bizalmas adatok kezelőjére és érintettjére, mint infokommunikációs rendszert használók munkáltatójára, mint információbiztonsággal kapcsolatos kötelezettségek alanyára, esetleg, mint az információbiztonsággal kapcsolatos bűncselekmény érintettjére;

(c) a természetes személyre, mint közigazgatási ügyfélre, fogyasztóra, elektronikusan szerződést kötő félre, információs társadalom, illetve a távközlési szolgáltatások igénybevevőjére, mint a személyes adat „érintettjére”, mint a munkaadójánál infokommunikációs rendszert használó munkavállalóra vagy az információs rendszer fejlesztőjére, esetleg, mint informatikai biztonsággal kapcsolatos bűncselekmény elkövetőjére vagy sértettjére.

Az infokommunikációs rendszert használó gazdálkodó szervezetek között meg kell különböztetni a közszolgáltató és a „felügyelt tevékenységet” végző, valamint az e kategóriákba nem tartozó gazdálkodó szervezeteket. E cégeket, illetve ágazatokat az informatikai biztonság tekintetében összefoglaló néven kritikus infrastruktúrának szokták nevezni. Kritikus infrastruktúraként kell kezelnünk *azon létesítményeket, eszközöket vagy szolgáltatásokat, amelyek működésképtelenné válása, vagy megsemmisülése a nemzet biztonságát, a nemzetgazdaságot, a közbiztonságot, a közegészségügyet vagy a kormány hatékony működését gyengítené, továbbá azon létesítményeket, eszközöket és szolgáltatásokat, amelyek megsemmisülése a nemzeti morált vagy a nemzet biztonságába, a nemzetgazdaságba, vagy a közbiztonságba vetett bizalmat jelentősen csökkentené.* Kritikus információs infrastruktúrák *azon az infokommunikációs létesítmények, eszközök vagy szolgáltatások, amelyek önmagukban is kritikus infrastruktúra elemek, továbbá a kritikus infrastruktúra*

elemeinek azon infokommunikációs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása, vagy megsemmisülése a kritikus infrastruktúrák működésképességét jelentősen csökkentené.

A Magyar Köztársaság kritikus információs infrastruktúrái közé tartoznak:

1. Az informatikai rendszerek és hálózatok;
2. Automatizálási, vezérlési és ellenőrzési rendszerek (SCADA, távmérő, távérzékelő és telemetriai rendszerek, stb.);
3. Internet szolgáltatás (infrastruktúra is);
4. Vezetékes távközlési szolgáltatások;
5. Mobil távközlési szolgáltatások;
6. Rádiós távközlés és navigáció;
7. Műholdas távközlés;
8. Műsorszórás;
9. Közigazgatási informatika és kommunikáció;
10. A kritikus infrastruktúrák létfontosságú infokommunikációs rendszerei.

Az infokommunikációs biztonság szempontjából azért kell megkülönböztetni a kritikus információs infrastruktúrákat a többi gazdálkodó szervezet infokommunikációs rendszereitől, mert amíg az utóbbiak elsősorban saját biztonságukat kockáztatják, ha gondatlanul járnak el, addig az előbbiek nem megfelelő működése sokkal szélesebb körben, jelentősebb károkat okozhat. Ezért velük kapcsolatban indokolt a többi gazdálkodó szervezetre vonatkozónál részletesebb infokommunikációs biztonsági követelmények betartásának és az ellenőrzési rendszerek kialakításának előírása és felügyelete.

Az infokommunikációs biztonsággal kapcsolatos kötelezettségeket azokra a szervezetekre is ki kell terjeszteni, amelyek az infokommunikációs rendszereket működtetik, vagy ezzel összefüggő szolgáltatásokat nyújtanak:

1. a távközlési szolgáltatók;
2. az internet-szolgáltatók (akik a távközlési szolgáltatók körébe tartoznak, de az infokommunikációs biztonság kérdéskörének különösen lényeges szereplői);
3. az információs társadalommal összefüggő szolgáltatásokat nyújtók;
4. a hitelesítés-szolgáltatók;
5. a távközlési és informatikai tanúsító szervezetek.

I.2. A védendő érdekek

A kritikus információs infrastruktúrák védelme a nemzetközi szabványokkal, a szövetségi rendszerekben előírtakkal összhangban az infokommunikációs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állásának, valamint a rendszer elemeinek sértetlensége és rendelkezésre állásának megőrzésére kell, hogy kiterjedjen.

A bizalmasság arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról. Ez számos jogot érint, így:

- **az államtitok és a szolgálati titok védelmét**, ami közérdek, tehát azt az infokommunikációs rendszerek használata során – a fokozottabb veszélyeztetéssel összhangban – fokozottan kell védeni;
- **a személyes adatok védelmét**, ami a természetes személyek alapvető joga, tehát azt minden, az infokommunikációs rendszerekkel adatkezelést végző szervezetnek garantálnia kell;
- **az üzleti titok és a magántitkok védelmét**, ami méltányolandó magánérdek, tehát elsősorban az érintetteknek kell a védelemről gondoskodnia, de ebben jogi és szakmai segítséget kell kapniuk.

A sértetlenség arra vonatkozik, hogy az adat fizikailag és logikailag teljes és bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik. A sértetlenség megőrzése:

- **az e-kormányzat, az e-önkormányzat területén** az elektronikus ügyintézés során különös szerepet kap, mert itt a köz- és az egyéni érdek azonos;
- **az e-szolgáltatások, az elektronikus gazdasági folyamatok** területén méltányolandó magánérdek, tehát elsősorban az érintetteknek kell a védelemről gondoskodnia, de ebben jogi és szakmai segítséget kell kapniuk.

A **rendelkezésre állás** az infokommunikációs rendszerek elemeinek a szükséges időben és időtartamra használhatóságára vonatkozik.

II. Biztonsági környezet – fenyegetések, kockázatok, kihívások

II.1. A hazai helyzet

Mind az államigazgatásban, mind a gazdaságban a rohamosan terjedő infokommunikációs alkalmazások (adatfeldolgozás, kommunikáció, média, stb.) hatékonysága, működőképessége, megbízhatósága – ezzel együtt az adott ágazat tevékenysége – alapvetően függ az infokommunikációs biztonság megfelelő kezelésétől, irányításától. Ezzel a fejlődéssel azonban újfajta veszélyek és fenyegetések is megjelennek.

A szervezetek, valamint infokommunikációs rendszereik egyre gyakrabban szembesülnek igen sokféle forrásból származó biztonsági fenyegetéssel, többek között gazdasági hírszerzéssel, ipari kémkedéssel, számítógépes csalással, szabotázzsal, vandalizmussal, vagy akár tűzzel vagy árvízzel, de egyre nagyobb fenyegetést jelent a terrorizmus új válfaja a kiberterrorizmus is.

A fejlett országok gyakorlatával ellentétben, az infokommunikációs biztonság helyzetére hazánkban jellemző, hogy súlya, kezelése nincs arányban a fontosságával, nincs egységesen alkalmazott módszertan, és nem kapcsolódik a fő nemzetközi irányzatokhoz.

Az infokommunikációs biztonság megoldatlan kérdései hosszú távon veszélyeztethetik a közigazgatás működőképességét és az infokommunikáció dinamikus továbbfejlődését. Ezek a hiányosságok nem mentesítik a felelősség alól az informatikai rendszerekben feldolgozott adatok védelméért felelős vezetőket, ugyanakkor megnehezítik, akadályozzák munkájukat.

Hazánkban hiányoznak a mai technológiai rendszerek szerepének, illetve veszélyeztetettségének megfelelő, az infokommunikációs biztonságra vonatkozó jogi keretek.

Az államtitokról és a szolgálati titokról szóló hatályos, 1995. évi LXV. törvény a módosításaival együtt sem harmonizál a NATO, EU, EURATOM és NYEU titokvédelmi előírásaival.

A szervezeti keretek Magyarországon szétforgácsoltak, és lefedetlen területek is vannak. A legtöbb fejlett országban az infokommunikációs biztonságot egy központi kormányszerv fogja össze (pl. UK: CESG, Németország: BSI, Franciaország: DCSSI, USA: NSA és NIST), a legtöbb – fejlett informatikai szinten álló – európai országban létezik ún. *InfoSec* hatóság. Magyarországon nincs központi felügyelet, irányítás. Több szervezet felelős a különböző részterületekért, és ezek döntő többsége is csak a minősített információk védelmére irányul, ezért maradnak lefedetlen részterületek.

Hazánkban az infokommunikációs biztonságra vonatkozó ajánlásokat tíz éve nem frissítették, azok elavultak. A közigazgatásban nincsenek érvényes informatikai biztonsági, infokommunikációs biztonsági követelmények, mert már a korábbi ajánlásokat sem tették kötelezővé. Bár születtek ajánlástervezetek, ezeket hivatalosan nem adták ki, így a felhasználókat az „állami akarat” kimutatásának hiánya visszatartja alkalmazásuktól.

Az állami szerepvállalás, támogatás is hiányzik a biztonsági szempontok érvényesítése, a biztonságos információs rendszerek kialakításának és fenntartásának támogatása területén.

II.2. Fenyegetések

Az internet az információs társadalmak alapvető infrastruktúrájává válik, és így az informatikai jellegű támadások megvalósítása is áttevődött az internetre, amely lehetővé teszi a nagy távolságokról történő támadásokat, viszonylagos anonimitást és védelmet biztosítva az elkövető számára.

A kritikus információs infrastruktúrákra nem fizikai jellegű fenyegetettségeit a támadó, valamint az elkövetés módja alapján csoportosíthatjuk. Az elkövető szándéka, rendelkezésére álló erőforrásai és szakértelme eltérő lehet. Veszélyeztető tényező lehet:

- a kiberterrorizmus;
- az információs hadviselés;
- a hírszerzés;
- az ipari kémkedés;
- a számítógépes bűncselekmények;
- a hanyagság és a felelőtlenség.

Az internet alapú támadások sajátos jellegei önmaguk megmagyarázzák azoknak gyakoriságát és hatását. Az internet lehetővé teszi a nagy távolságokról történő támadásokat, amely magasabb fokú anonimitást és védelmet biztosít az elkövető számára. Ez a sajátosság csökkenti a jogszabályok hatékonyságát is. Számos esetben a támadásokat a nemzeti határokon túlról intézik. Más infokommunikációs jellegű támadásokhoz hasonlóan, az internetes támadások során is gyakran használják fel a számítógépeket bizonyos eljárások automatikus ismétlődésére, mint például a szótár alapú kereső programok jelszavak feltörésére, vagy vírusok, melyek korlátlanul replikálják önmagukat. Ez a sajátosság kiegészítheti az egyén szakértelmét globális kihatással járó infrastruktúra megtámadására is. Ilyen esetben a bekövetkezett hatás nincs összefüggésben a támadó rendelkezésére álló erőforrásokkal. Figyelembe veendő, hogy az előre megírt, automatizált támadási eszközök egyre szélesebb körben elérhetőek az interneten, s olyan személyek által is használhatóvá válnak, akik nincsenek tisztában magával az eszközzel vagy a hatásukkal.

III. Célok

A Magyar Köztársaság nemzeti biztonsági stratégiájával (2073/2004. (IV. 15.) Korm. határozat) összhangban az infokommunikációs biztonsági stratégia általános célkitűzése a nemzet biztonságának megőrzése azáltal, hogy megakadályozza, vagy elviselhető mértékűre csökkenti a kritikus információs infrastruktúrák elleni sikeres támadások lehetőségét,

valamint a bekövetkezett támadások hatását a lehető legkisebbre csökkenti. Ennek érdekében a következő célokat határozza meg:

III.1. A kritikus információs infrastruktúrák elleni támadások hatékony megelőzése

Szükséges, hogy az ország működéséhez létfontosságú információs infrastruktúrák védelme készüljön fel a támadások megelőzésére a védendő kör beazonosításával és felkészítésével, valamint a potenciális támadások észlelésével és a támadók jogi-technikai elrettentésével.

III.2. A kritikus információs infrastruktúrák elleni támadások hatékony kivédése

Szükséges, hogy az ország működéséhez létfontosságú információs infrastruktúrák védelme képes legyen a támadások elhárítására megfelelő reagáló-kapacitások kialakításával.

III.3. A kritikus információs infrastruktúrák elleni támadások hatékony kezelése

Szükséges, hogy az ország működéséhez létfontosságú infrastruktúrák védelme terjedjen ki a bekövetkezett támadások hatásának csökkentésére, a helyreállítási idő minimalizálására, valamint a támadók beazonosítására, elfogására.

IV. Feladatok

IV.1. Állami koordináció

A kritikus információs infrastruktúrák védelmének alapvető eszköze a – más államokban már létrehozotthoz hasonló – kormányzati koordináció. Ennek elsődleges feladata:

- a nemzeti infokommunikációs biztonsági stratégiában foglaltak megvalósítása;
- az állami, önkormányzati és a magánszektor koordinációja és integrációja;
- a nemzeti infrastruktúra sérülékenységeinek, fenyegetettségeinek feltérképezése;
- a nemzeti infrastruktúra védelmi terv elkészítése.

Rövidtávon a fenti feladatok ellátásához szükséges koordinációt a Miniszterelnöki Hivatal Elektronikus Kormányzati Központja láthatja el, a következő szervezetek bevonásával:

- Gazdasági és Közlekedési Minisztérium;
- Igazságügyi és Rendészeti Minisztérium;
- Nemzeti Hírközlési Hatóság;

- Katasztrófavédelmi Főigazgatóság;
- Országos Rejtjelfelügyelet;
- Nemzeti Biztonsági Felügyelet.

A nemzetközi gyakorlatot alapul véve közép- és hosszútávon a kormányzati koordinációhoz szükséges egy kormányzati Információ Biztonsági Felügyelet, az úgynevezett **InfoSec Hatóság** felállítása, amely:

- gondoskodik az infokommunikációs rendszerek és eszközök – különösen a minősített adatot kezelő rendszerek és eszközök – biztonsági követelményeinek, szabványainak és ajánlásainak kidolgozásáról (honosításáról) és karbantartásáról;
- ellátja az infokommunikációs eszközök (termékek) infokommunikációs biztonsági tanúsításának felügyeletét, a tanúsítás alapján kiadja az infokommunikációs rendszerek és eszközök infokommunikációs biztonsági minősítését;
- ellátja az infokommunikációs rendszerek vagy eszközök biztonsági vizsgálatát végző személyek és szervezetek működésének engedélyezését;
- ellátja a központi közigazgatási szervek és a helyi önkormányzati közigazgatási szervek hitelesítő szolgáltató feladatát;
- felügyeli az infokommunikációs biztonsági (vészjelző és beavatkozó) központot;
- az államtitokról és a szolgálati titokról szóló törvény hatálya alá tartozó minősített adatot (továbbiakban: minősített adat) kezelő infokommunikációs rendszerek létesítését, működtetését és megszüntetését engedélyezi;
- ellátja a minősített adatot tartalmazó infokommunikációs rendszerek infokommunikációs biztonsági szempontból történő felügyeletét;
- kivizsgáltatja a közigazgatás, az állami irányítás alatt álló szervezetek, a stratégiai feladatokat ellátó szervezetek infokommunikációs rendszerei biztonságával kapcsolatos eseményeket.

IV.2. Monitorozás és reagálás

A 2001. szeptember 11-i terrortámadás során a nyugati világ felismerte, hogy szüksége van olyan központokra, amiknek a segítségével képes a lehető leggyorsabban reagálni az egyes vészhelyzetekre. Ennek alapján Magyarországon a Nemzeti Hírközlési Hatóság keretei közt megalakult az Országos Informatikai és Hírközlési Főügyelet (OIHF), illetve a kormányzat 2005-ben létrehozta a Puskás Tivadar Közalapítvány keretében a CERT-Hungary Központot, amelynek feladatául szabta a kormányzati és a kritikus információs infrastruktúrák

védelmét, valamint a hálózatbiztonsági tudatosság növelését. 2006 januárjában az OIHF ügyeleti szolgálata kiszervezésre került a CERT-Hungary-hoz, azóta megtörtént a két ügyelet üzemeltetésének, ügyeleti tevékenységének és jelentési rendjének összehangolása. A CERT-Hungary akkreditált tagja a hálózatbiztonsági központok európai (TF-CSIRT) és nemzetközi (FIRST) szervezeteinek, valamint részese a kormányzati hálózatbiztonsági központokat, döntéshozókat és számítógépes bűnüldöző szerveket tömörítő International Watch and Warning szervezetnek. Emellett a CERT-Hungary tevékeny részt vállal a hazai internetes támadások elhárításában, 2006 decemberében a Bankszövetség és a Nemzeti Nyomozó Iroda felkérésére szüntette meg a magyar bankokat külföldről támadó adathalász honlapokat.

A CERT-Hungary további kormányzati támogatása javasolt, részére feladatként kell szabni:

- a kritikus infrastruktúrához tartozó elektronikus hírközlési és informatikai rendszerek védelmének támogatását hálózatbiztonsági felügyelettel és incidenskezeléssel;
- a nyílt hálózati rendszerekhez kapcsolódó rendszereket (internet) ért támadások figyelését, felismerését, és a kritikus infrastruktúrákat üzemeltetők figyelmeztetését;
- az internet biztonsági kockázatainak folyamatos figyelését és értékelését;
- a kritikus információs infrastruktúrák védelemhez kapcsolódó tevékenységének kialakítását, fejlesztését és koordinációját;
- az infokommunikációs rendszerek vagy eszközök biztonsági vizsgálatával, a kritikus infrastruktúrához tartozó infokommunikációs rendszerek biztonságával kapcsolatos oktatások, a szükséges továbbképzések és vizsgáztatások lebonyolítását;
- a terrorizmus és a számítógépes bűnözés felderítésében a nemzetbiztonsági szolgálatokkal és a rendőrséggel történő együttműködést.

Utóbbi feladat érdekében szükséges, hogy a Nemzetbiztonsági Szakszolgálat és a Nemzeti Nyomozó Iroda, valamint a CERT-Hungary operatív kapcsolatai intézményesüljenek a nemzetközi gyakorlatnak megfelelően.

IV.3. Jogszabályok, szabványok és ajánlások

IV.3.1. Jogszabályok

A jelenlegi egyenetlen és szétszórt szabályozás helyett szükséges egy egységes és összetett szabályozási rendszert kialakítani törvényi és rendeleti szinteken.

Első lépésként a Miniszterelnöki Hivatal Elektronikus Kormányzati Központját kell kijelölni a közigazgatás területén egységesen érvényes infokommunikációs biztonsági

jogszabályi, technológiai követelmények meghatározására és felügyeletére, valamint az infokommunikációs technológiákkal szemben fellépő veszélyek elleni védekezésre alkalmas biztonsági szabványok, rendszerek kialakítására, tanúsítására és alkalmazására.

A titokvédelemben a papíralapú minősített adatok védelmével azonos hangsúlyt kell kapnia az infokommunikációs rendszerekben kezelt minősített adatok védelmének. A védelmi előírásoknak összhangban kell lenniük a NATO, az EU, az EURATOM és a NYEU titokvédelmi előírásaival és elvárásaival.

Rendelkezni kell továbbá az infokommunikációs rendszerek, eszközök biztonsági vizsgálatainak szabályairól, az állami irányítás és felügyelet – az EU irányelveivel összhangban történő – megoldásáról.

IV.3.2.Szabványok és ajánlások

A nemzetközi szervezetek által kidolgozott szabványok, standardok átvétele által a nemzetközi szinten kidolgozott és használt infokommunikációs biztonsági értékelési, minősítési rendszerek bekerülhetnek a magyar szabályozás rendszerbe, a külföldön elvégzett értékelés, minősítés értelmezhető, alkalmazható lesz Magyarországon is.

A kritikus infrastruktúrához tartozó infokommunikációs rendszerek esetében törekedni kell arra, hogy értékelt informatikai termékeket és rendszereket alkalmazzanak. Ehhez vagy az ISO/IEC 15408 (Common Criteria) szerinti tanúsítvánnyal rendelkező informatikai termékek beszerzése és felhasználása szükséges (az ilyen termékek további értékelésére nincs szükség), vagy amennyiben az adott termékkörben nincs az ISO/IEC 15408 szerinti értékelés, de biztonsági szempontból értékelt termék használata indokolt, úgy azt egyszerűsített eljárás, a Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS) keretében is értékelni lehessen. Ezért szükséges az ISO/IEC 15408 (Common Criteria) szabvány szerinti tanúsítványok hazai kibocsátásának lehetőségének megteremtése.

A kritikus információs infrastruktúrákat üzemeltető szervezetek kapcsán szükséges, hogy a felhasználók világosan megfogalmazhassák az elvárásaikat a fejlesztés, üzemeltetés során. Ehhez az ISO/IEC 27000 nemzetközi szabványsorozatra épülő irányítási és követelményrendszer, a Magyar Informatikai Biztonság Irányítási Keretrendszer (MIBIK) bevezetése alkalmat ad. Az egységes elveken nyugvó előírások alapján elkészíthetők a különböző szervezeteknél az informatikai biztonság alapdokumentumai (az információbiztonsági politika, az infokommunikációs biztonsági stratégia és az Infokommunikációs Biztonsági Szabályzat). Emellett a keretrendszer segítséget ad a

biztonságos működéshez szükséges szervezeti struktúra, a személyi, a fizikai és az infokommunikációs védelem kialakításához és ellenőrzéséhez.

IV.4. Az informatikai rendszerekbe vetett bizalom erősítése, az információbiztonsági tudatosság és ismeretek fejlesztése

A kritikus információs infrastruktúrák védelme során figyelembe kell venni azt a tényt, hogy biztonsági előírásaik csak akkor hatékonyak, ha felhasználóik alkalmazzák őket. Ezért fontos cél, hogy minden szereplőben tudatosuljanak a támadások korán felismerhető jelei és az eredményes támadások súlyossága. Folyamatossá kell tenni a szakemberek számára a biztonsági továbbképzéseket, valamint az egyéni felhasználó számára a felvilágosítást, valamint az infokommunikációs biztonsággal kapcsolatos ismeretek oktatását.

IV.5. A nemzetközi szövetségi rendszer használata és fejlesztése, a hazai üzleti, civil és akadémiai szféra bevonása

A kritikus információs infrastruktúrák védelmi feladatainak ellátását a kritikus információs infrastruktúrák nemzetközi beágyazottsága és valamint magántulajdon túlsúlya együttesen befolyásolja. Ezért elengedhetetlen, hogy a védelem kialakításánál a hazai üzleti, civil és akadémiai szféra bevonásra kerüljön, továbbá a kritikus információs infrastruktúrák védelmére szakosodott nemzetközi szervezetekben Magyarország aktívan vegyen részt.

KÖVETKEZTETÉSEK

A Magyar Köztársaság kritikus információs infrastruktúráira vonatkozó védelmi javaslatok összeállításánál az egyik oldalról a semmiből kellett építkezni. **Alapvető intézkedések is hiányoznak a kritikus információs infrastruktúrák védelméhez.** Az utóbbi években jelentősen megváltoztak a biztonsági fenyegetések, kockázatok, amelyekre nem vagyunk felkészülve, ugyanakkor megszűnt az állami irányítás és támogatás, beavatkozás a biztonság területén.

A releváns nemzetközi és hazai előírások és ajánlások áttekintése során **jelentős lemaradásokat állapítottam meg**. Az Európai Unió pályázati rendszere miatt Magyarország szempontjából fontos lenne a kutatóintézetek, a kritikus infrastruktúra üzemeltetők, valamint az állami szféra minél széles körben történő tájékoztatása és pályázati hajlandóságuk

elősegítése, különös tekintettel a jelenlegi költségvetési lehetőségekre, amelyek a kritikus infrastruktúrák védelmi programjainknak a teljes körű finanszírozását nem teszi lehetővé.

Tekintettel arra, hogy a kritikus infrastruktúrák védelmének biztosítása egyaránt állami és üzemeltetői érdek, ezért úgy gondolom, hogy fel kell készülni az európai uniós források felhasználására, és meg kell teremteni a védelmi intézkedések finanszírozásának új konstrukcióját, a PPP kialakítását, a magánszféra bevonását.

A kritikus információs infrastruktúrák védelméhez kapcsolódó területen sok az elmaradás, a hiányos, ellentmondó szabályozás, és ennek csak egy része magyarázható az anyagi lehetőségek hiányával. Ez a terület elhanyagoltságát, gazdátlanságát mutatja. Az infokommunikációs infrastruktúrák és rendszerek védelmére irányuló aktuális előírások, ajánlások is hiányosak, érthetetlen okokból az elkészült és szakmailag elfogadott ajánlástervezetek (MIBÉTS, MIBIK) nem emelkednek az *ajánlás* szintjére. A kritikus információs infrastruktúrák szabályozása Magyarországon még kialakulatlan, ezért szükséges az egyes részterületek átfogó vizsgálata, elemzése, és a kérdéskör törvényi és rendeleti szintű szabályozása – ez lehetőséget teremtene a kapcsolódó biztonsági, védelmi igazgatási kör rendezésére is.

Az államigazgatási szervezetek tevékenységéről könnyű hibás képet alkotni annak, aki nem közvetlen részese e feladatoknak. Éppen ezért – az általam feltárt hiányosságok valóságosságának alátámasztására – hazánk biztonságpolitikáját és annak megvalósulását jól ismerő szerző, Dr. Szenes Zoltán nyá. altábornagy írását idézem:

„Éppen ezért egy olyan biztonságfelfogásra és cselekvési programra van szükség, amely a magyar kormányzati és közigazgatási rendszerben „leképezhető”, működtethető, ahol a feladatok, a felelősség és a kompetencia egyértelműen szabályozott. Mivel a hivatalos biztonságfelfogás túlságosan általános, differenciálatlan és diffúz, a biztonsági kockázatok kommunikációs és kormányzati-közigazgatási kezelése is hasonló.

... a biztonság „puha” aspektusai (gazdasági biztonság, információs biztonság stb.) teljesen esetlegesen jelennek meg az elméleti és gyakorlati szférában. A nemzeti biztonság komplex felfogásának elmélete és egységes kormányzati praxisa pedig teljesen hiányzik. ... a Magyarországon kialakult intézményi biztonsági rendszer egyes veszélytípusokra „szakosodott”, még csak nem is tárca-, hanem ágazati szinten „manifesztálódott”. Ahogy az egyes külső vagy belső kihívások, kockázatok „komplikálódnak”, már nem lehet őket a régi, hagyományos szerkezeti rendszerben megválaszolni, és egyre több, különböző rendeltetésű, irányítású, működési filozófiájú és képességű szervezet bevonására van szükség. ... A

kormányzati koordináció elégtelenségét mutatja a biztonsági dokumentumok „karbantartásának" hiánya, az ágazati stratégiák kidolgozásának elégtelensége is." [97]

Bár a kisszámú szakember-gárda a maga részéről mindent megtesz a feladatainak szakszerű és maradéktalan ellátása érdekében, ez a politikai vezetés támogatása nélkül kevés eredménnyel kecsegtet. Véleményem szerint a magyar közigazgatás szakmailag kész és képes lenne az Európai Unió és a NATO elvárásaival, ajánlásaival összhangban a Magyar Köztársaság kritikus információs infrastruktúráinak védelmi kérdéseit megoldani. Ehhez azonban hiányzik az egyértelmű és következetes állami-politikai akarat és így a támogatás is.

Mint már korábban megállapítottam az önszerveződő, társadalmi alapokon (is) működő hálózatbiztonsági szervezetek egyre nagyobb szerepet kapnak a kritikus információs infrastruktúrák védelmében. **Megítélésem szerint a CERT-ek ezt a tevékenységet valóban képesek jól ellátni**, különösen a monitorozás és az információ-megosztás (biztonságkultúra fejlesztése) területén. A CERT-HUNGARY a nehéz, sokszor visszás hazai viszonyok között is jól teljesít, és ezt ki kell használni a kritikus információs infrastruktúra védelme során.

A hiányosságokat minél előbb fel kell számolni, és ezt követően lehet a NATO és az Európai Unió kritikus infrastruktúra, kritikus információs infrastruktúrák védelmi programjaiban részt venni. Ehhez szerencsére rendelkezésre áll sok külföldi minta, dokumentum, amelyek alapján könnyebben lehet a felzárkózást végrehajtani.

Az infokommunikációs infrastruktúrák közötti számottevő különbség miatt a tervezés során külön-külön kell vizsgálni az egymástól függő viszonyban lévő infrastruktúrákat, azoknak az infokommunikációs hálózatra gyakorolt hatását, kockázatait.

A kritikus információs infrastruktúrák védelme érdekében egy **nemzeti program keretében** törvényben és alacsonyabb szintű jogszabályban **rögzíteni kell** a **kritikus infrastruktúrák védelmével kapcsolatos feladatokat** (ideértve a titokvédelemi hiányosságok, vagy a nemzeti biztonsági stratégia részstratégiáinak pótlását is) és **felelősségeket**, meg kell teremteni az érintett szereplők együttműködési lehetőségét (és kényszerét). A kormányzati, védelmi, gazdasági és társadalmi szervezetek közötti megfelelő – gazdasági és jogszabályi alapon történő – együttműködést ki kell alakítani.

Az EU és a NATO ajánlásait és dokumentumait, az infokommunikációs rendszerek biztonságával kapcsolatos ajánlásokat alkalmazni kell. Meg kell teremteni a kritikus információs infrastruktúrák védelme négy pillérét: a megelőzés és korai figyelmeztetés, az észlelés, a reagálás és a krízismenedzsment egységes, államilag támogatott és koordinált működtetését.

Mindezek alapján, a feltárt hiányosságok egy részének a megszüntetése érdekében **javaslatot tettem a legfontosabb állami szintű szabályozási feladatokra**, és ezek egyikét, a **Magyar Köztársaság infokommunikációs biztonsági stratégiáját kidolgoztam**.

ÖSSZEGZETT KÖVETKEZTETÉSEK

- Az Európai Unió, a NATO és több ország, köztük a Magyar Köztársaság kritikus infrastruktúra, kritikus információs infrastruktúra fogalma, illetve elemeinek meghatározása alapján megállapítottam, hogy a kritikus információs infrastruktúra elemeinek jó meghatározásához **először a fogalomrendszert kell rögzíteni**. A kritikus infrastruktúra elemeinek meghatározása során **az egyes országok fejlettségét, gazdasági és kulturális strukturáltságát, értékrendjét, gondolkodás módját is vizsgálni kell.**

- Megvizsgáltam az Európai Unió, a NATO valamint néhány fejlett infrastruktúrával rendelkező ország kritikus infrastruktúrákra és kritikus információs infrastruktúrákra vonatkozó fogalmi meghatározásait. Ezek elemzése, illetve a hazai meghatározásokkal való összehasonlítása után **azt a következtetést vontam le, hogy a hazai kritikus infrastruktúra és kritikus információs infrastruktúra fogalmak nem megfelelőek. Ezért meghatároztam a Magyar Köztársaság kritikus infrastruktúra fogalmát, a kritikus infrastruktúrák alágazatait és felelőseit,** valamint a **Magyar Köztársaság kritikus információs infrastruktúra fogalmát** és azok **alágazatait.**

- Megvizsgáltam és elemeztem a kritikus információs infrastruktúrákat fenyegető veszélyeket. Külön vizsgáltam a fizikai dimenzióból, és külön az információs dimenzióból érkező lehetséges fenyegetéseket. **Ezek alapján megállapítottam a kritikus információs infrastruktúrákat az információs dimenzióból fenyegető veszélyeket.**

- Megvizsgáltam az Európai Unió, a NATO és néhány fejlett ország e téren megvalósított védelmi gyakorlatát. Az EU határozatait, irányelveit és javaslatait feldolgozva arra a **következtetésre jutottam**, hogy a kritikus információs infrastruktúrák védelme tekintetében **komoly előrelépések történtek**. A nemzetközi helyzet elemzése után azt a következtetést vontam le, hogy az egyes országok politikai vezetése megértette a problémát és **megteremtette a szükséges jogszabályi hátteret** a védelem érdekében.

- A bemutatott Észt-Orosz konfliktust elemezve, azt a következtetést vontam le, hogy egy az információs dimenzióból érkező támadás komoly károkat okozhat egy fejlett infrastruktúrával rendelkező országnak. A bemutatott példa jól rávilágít arra a tényre, hogy a **védelem terén elengedhetetlenül fontos a megelőzés, a jogszabályoknak, szabványoknak, ajánlásoknak megfelelően felépített, megfelelő tartalékolással rendelkező biztonságos rendszerek kialakítása.**

- A nemzetközi tapasztalatok elemzése alapján **megállapítottam**, hogy **az önszerveződő, társadalmi alapokon (is) működő hálózatbiztonsági szervezetek egyre nagyobb szerepet kell, hogy kapjanak a kritikus információs infrastruktúrák védelmében**, különösen a monitorozás és az információ-megosztás (biztonságkultúra fejlesztése) területén.

- A Magyar Köztársaság kritikus információs infrastruktúráinak védelmét elemezve **megállapítottam**, hogy hazánkban **alapvető intézkedések is hiányoznak a kritikus információs infrastruktúrák védelméhez.** Az utóbbi években jelentősen megváltoztak a biztonsági fenyegetések, kockázatok, amelyekre nem vagyunk felkészülve, ugyanakkor megszűnt az állami irányítás és támogatás, beavatkozás a biztonság területén. Mindezeket figyelembe véve **jelentős lemaradásokat állapítottam meg** a területen.

- Megállapítottam, hogy a hiányosságok megszüntetése, valamint a minél hatékonyabb védelem megteremtése érdekében egy **nemzeti program keretében** törvényben és alacsonyabb szintű jogszabályban **rögzíteni kell** a **kritikus infrastruktúrák védelmével kapcsolatos feladatokat** (ideértve a titokvédelemi hiányosságok, vagy a nemzeti biztonsági stratégia részstratégiáinak pótlását is) és **felelősségeket**, meg kell teremteni az érintett szereplők együttműködési lehetőségét (és kényszerét). A kormányzati, védelmi, gazdasági és társadalmi szervezetek közötti megfelelő – gazdasági és jogszabályi alapon történő – együttműködést ki kell alakítani.

- Mindezek alapján, a feltárt hiányosságok megszüntetése érdekében **javaslatot tettem a legfontosabb állami szintű szabályozási feladatokra**, és ezek egyikét, a **Magyar Köztársaság infokommunikációs biztonsági stratégiáját kidolgoztam**.

ÚJ TUDOMÁNYOS EREDMÉNYEK

1. Megvizsgáltam a hazai kritikus infrastruktúra és kritikus információs infrastruktúra meghatározásokat. Megállapítottam, hogy azok nem megfelelőek, ezért elemezve a különböző nemzetközi szervezetekben és országokban meglévő kritikus infrastruktúra és kritikus információs infrastruktúra fogalmakat, azokból következtetések levonva **meghatároztam a hazai kritikus infrastruktúrák és kritikus információs infrastruktúrák fogalmát, valamint mindkét esetben azok alágazatait**.

2. Megvizsgáltam, hogy milyen veszélyek fenyegetik a kritikus infrastruktúrákat és a kritikus információs infrastruktúrákat. Ezek alapján elemeztem a különböző nemzetközi szervezetek és országok e veszélyek ellen tett lépéseit, majd **mindezek alapján feltártam a nemzetközi védelmi megoldásokat.**

3. Elemeztem a hazai kritikus infrastruktúrák és kritikus információs infrastruktúrák védelmének helyzetét, amely alapján mind a fenyegető veszélyek terén, mind a nemzetközi téren tapasztalt eddigi védelmi lépésekhez képest komoly hiányosságokat és lemaradásokat állapítottam meg. Ezért **kidolgoztam a minimálisan szükséges parlamenti és kormányzati feladatokat**, amely elengedhetetlenül szükségesek a **Magyar Köztársaság kritikus információs infrastruktúrái védelmének** euró-atlanti kompatibilitásához.

4. A kritikus infrastruktúrák és kritikus információs infrastruktúrák védelme terén megállapított hazai hiányosságok megszüntetése érdekében **kidolgoztam** a védelem egyik részterületére a **Magyar Köztársaság infokommunikációs biztonsági stratégiáját.**

AJÁNLÁSOK

1. A doktori (PhD) értekezésemben megfogalmazottakat javaslom felhasználni a területre vonatkozó stratégiák, programok, jogszabályok és ajánlások megalkotásában, aktualizálásában, különös tekintettel az alábbiakra:
   - a nemzeti kritikus infrastruktúrák védelmi program megalkotása;
   - a kritikus infrastruktúrák védelmi követelményeiről szóló törvény megalkotása;
   - a honvédelmi törvény aktualizálása;
   - a titokvédelmi törvény aktualizálása;
   - az infokommunikációs biztonsági stratégia kiadása;
   - az infokommunikációs rendszerek biztonságával kapcsolatos ajánlások, módszertani segédanyagok aktualizálása (elkészítése).

2. Javaslom értekezésemet felhasználni a kritikus információs infrastruktúrák, illetve a kapcsolódó szakterületeken folyó egyetemi (főiskolai) alap, mester és doktori képzésben tananyagként.

3. Javaslom értekezésem – információs infrastruktúrák védelmével kapcsolatos – jogszabályokat, ajánlásokat áttekintő és összefoglaló részeit, az általam javasolt stratégiával együtt felhasználni az információbiztonsági szakemberek különböző tanfolyami képzéseiben, illetve továbbképzéseiben.

FELHASZNÁLT IRODALOM

[1] „Lord Hansard text” (241209-22), www.publications.parliament.uk, 2004. december 09.

[2] 1/2007. (III.29.) Kormányzati Koordinációs Bizottság határozat a katasztrófavédelemmel összefüggő 2007. évi feladatokról

[3] 1995. évi LXV. törvény az államtitokról és a szolgálati titokról

[4] 2004. évi CV. törvény a honvédelemről és a Magyar Honvédségről

[5] 2046/2007 (III. 19.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól szóló 2112/2004. (V. 7.) Korm. határozat módosításáról

[6] 2073/2004. (IV. 15.) Korm. határozat a Magyar Köztársaság nemzeti biztonsági stratégiájáról

[7] 2112/2004. (V.7.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól

[8] 2151/2005. (VII. 27.) Korm. határozat a Terrorizmus Elleni Akcióterv felülvizsgálatáról

[9] 2236/2003. (X. 1.) Korm. határozat a Magyar Honvédség 2004-2013 közötti időszakra vonatkozó átalakításának és új szervezeti struktúrájának kialakításáról

[10] 27/2004. (X. 6.) IHM rendelet az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségéről

[11] A CERT-Hungary honlapja felhasználók számára, www.biztonsagosinternet.hu

[12] A CERT-Hungary honlapja szakemberek számára, www.halozatbiztonsag.hu

[13] A kritikus infrastruktúrák védelme – társadalmi feladat vagy üzleti lehetőség?. Informatikai Vállalkozások Szövetsége közleménye, Budapest, 2007.08.09. http://www.ivsz.hu/engine.aspx?page=showcontent&content=hirek_mentainfo_070809

[14] A Magyar Hírlap 2007.06.04-i cikke. http://www.magyarhirlap.hu/cikk.php?cikk=130135

[15] A Magyar Nemzet Online adatai. http://www.mno.hu/docfiles/0707/dhgtabla.pdf

[16] Availability and Robustness of Electronic Communications Infrastructures, “The ARECI Study”, Final Report, European Commission Information Society and Media Directorate-General, Brussels – Luxembourg, 2007. március, http://ec.europa.eu/idabc/servlets/Doc?id=28182

[17] Az Európai Bizottság közleménye: i2010: európai információs társadalom a növekedésért és a foglalkoztatásért, Európai Közösségek Bizottsága, Brüsszel COM(2003) 784, 2005.01.06.

[18] Az Európai Parlament 2007. május 24-i állásfoglalása Észtországról, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2007-0215&language=HU&ring=B6-2007-0220

[19] Az Európai Parlament és a Tanács 460/2004/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról, 2004. március 10.

[20] Az SG.hu 2007.05.18-i cikke, http://www.sg.hu/cikkek/52426

[21] BALÁZS István et al.: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS), 1-12 kötet, Információs Társadalom Koordinációs Tárcaközi Bizottság ajánlástervezet, Budapest, 2004.

[22] BIAŁAS, Andrzej: Information Security Systems vs. Critical Information Infrastructure Protection Systems – Similar and Differences, In. Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T.: Proceedings of the International Conference on Dependability of Computer Systems, DepCoS-RELCOMEX 2006, IEEE Computer Society Los Alamitos, Washington, Tokyo, ISBN 0-7695-2565-2, p.60-67.

[23] BIRKÁS László, MUHA Lajos, SUBA Ferenc, SZEKERES Balázs: Miniszterelnöki Hivatal Elektronikuskormányzat Központ Informatikai Biztonsági Központ koncepció – tanulmány, Puskás Tivadar Közalapítvány, Budapest, 2006. december

[24] BOTZ László: A magyarországi biztonsági rendszer és elemeinek helyzete és felkészültsége a várható fenyegetések elhárítására tanulmány, http://www.mtaki.hu/docs/all_in_one/botz_laszlo_mo_biztonsagi_rendszere.pdf

[25] BUKOVICS István - VAVRIK Antal: Infrastruktúrák kockázata és biztonsága: kritikai problémaelemzés, Hadmérnök I. Évfolyam 3. szám – 2006. december, http://zrinyi.zmne.hu/hadmernok/archivum/2006/3/2006_3_bukovics.html

[26] BUKOVICS István: Logikai „nemvalószínűségi" kockázatelemzés, Hadtudomány XVI. évf 2006/3

[27] Centre of the Protection of National Infrastructure honlapja, http://www.cpni.gov.uk/productsServices.aspx

[28] COM(2006)0787 Javaslat A Tanács irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről, Brüsszel, 2006

[29] COM(2006)786 A Bizottság közleménye a létfontosságú infrastruktúrák védelmére vonatkozó európai programról, Brüsszel, 2006

[30] Communication from the Commission to the Council and the European Parliament, Brussels, 20.10.2004. COM(2004) 702 Final, Critical Infrastrucure Protection in the fight against terrorism

[31] Control Objectives for Information and related Technology (COBIT), http://www.isaca.org/cobit

[32] Critical Foundations Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, Washington, 1997. október

[33] Critical Information Infrastructure Research Co-ordination (CI2RCO) Projekt weblapja, http://www.ci2rco.org

[34] CSÍK B. et al., Az informatikai biztonság fogalmainak gyűjteménye, BME GTK, Budapest, 2003

[35] BELL, David E. – LAPADULA, Leonard J.: "Secure Computer Systems: Mathematical Foundations," ESD-TR-73-278, Vol. I, Electronic Systems Division, Air Force Systems Command, Hanscom AFB, Bedford, MA 01731, 1973, http://www.albany.edu/acc/courses/ia/classics/belllapadula1.pdf

[36] Department of Defense Standard (DoD 5200.28-STD): Department of Defense Trusted Computer System Evaluation Criteria, 1985, http://csrc.nist.gov/publications/history/dod85.pdf

[37] DÉRI Zoltán et al.: Az informatikai biztonság irányításának követelményrendszere – Információs Társadalom Koordinációs Tárcaközi Bizottság ajánlástervezet, Budapest, 2004.

[38] DÉRI Zoltán et al.: Az informatikai biztonság irányításának vizsgálata (módszertan) – Információs Társadalom Koordinációs Tárcaközi Bizottság ajánlástervezet, Budapest, 2004.

[39] Euro-Atlantic Partnership Council Senior Civil Emergency Planning Committee: Critical Infrastructure Protection – Concept Paper, EAPC(SCEPC)D(2003)15, 2003.11.10., http://www.ndc.nato.int/news/sc106_et_ante/cip_eapc/EAPC(CPC)D(2003)15 Road Map F inal incl FR.pdf

[40] Európai Gazdasági és Szociális Bizottság vélemény – Tárgy: A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: A biztonságos információs társadalomra irányuló stratégia: "párbeszéd, partnerség, felvértezés és felelősségvállalás", COM(2006) 251 final, 2007.04.28.

[41] Európai Unió Tanácsának Biztonsági Szabályzata (2001/264/EK)

[42] FM 100-6, Information Operations. Department of the Army, Washington DC, 1996.

[43] GERENCSÉR András: Informatikai és információvédelmi nemzeti biztonsági stratégia – előadás az Információs Társadalom Koordinációs Tárcaközi Bizottság Informatikai Biztonsági Albizottság, Budapest 2005. 02. 28-i ülésén http://www.itktb.hu/Resource.aspx?ResourceID=docstorefile&f=899&t=stored

[44] Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation, COM(97) 623, Európai Közösségek Bizottsága, Brüsszel, 1997.12.03.

[45] HAIG Zsolt: Az információbiztonság komplex értelmezése, Robothadviselés 6. tudományos szakmai konferencia, 2006. november 22.

[46] HAIG Zsolt: Az információs társadalmat fenyegető információalapú veszélyforrások, In. Hadtudomány, Budapest, 2007.

[47] HAIG Zsolt-KOVÁCS László-MAKKAY Imre-SEEBAUER Imre-VASS Sándor-VÁNYA László: Az információs társadalom veszélyforrásai. A kormányzat szerepe a védelem és ellentevékenység műszaki és szervezeti megoldásaiban. Tanulmány. MEH Informatikai Kormánybiztosság, 2002.

[48] HAIG Zsolt-VÁRHEGYI István: Hadviselés az információs hadszíntéren, Zrínyi, Budapest, 2005.

[49] Homeland Security Presidential Directive/ HSDP-7, 2003. december 17., Subject: Critical Infrastructure Identification, Prioritization, and Protection, http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

[50] http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm

[51] http://www.cramm.com

[52] http://www.ddsi.org/htdocs/DDSI-F/main-fs.htm

[53] http://www.ddsi.org/htdocs/Documents/CR/DDSI_International_organisations.pdf

[54] http://www.mno.hu/docfiles/0707/dhgtabla.pdf

[55] http://www.niscc.gov.uk/niscc/aboutCNI-en.html

[56] International CIIP handbook 2006 Myriam Dunn and Victor Mauer (eds.) Swiss Federal Institute of Technology (ETH Zurich)

[57] ISO/IEC 13335-1:2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management

[58] ISO/IEC 15408-1:2005 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

[59] ISO/IEC 15408-2:2005 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements

[60] ISO/IEC 15408-3:2005 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements

[61] ISO/IEC 17799:2000 Information technology – Code of practice for information security management, withdrawn standard

[62] ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management

[63] ISO/IEC 20000-1:2005 Information technology – Service management – Part 1: Specification

[64] ISO/IEC 20000-2:2005 Information technology – Service management – Part 2: Code of practice

[65] ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

[66] ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management

[67] ISO/IEC 27006:2007 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

[68] ISO/IEC CD 27004 Information technology – Security techniques – Information security management measurements, standard under development

[69] ISO/IEC FCD 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary, standard under development

[70] ISO/IEC FCD 27005 Information technology – Security techniques – Information security risk management, standard under development

[71] ISO/IEC FCD 27011 Information technology – Security techniques – Information security management guidelines for telecommunications, standard under development

[72] ISO/IEC TR 13335-2:1997 Information technology – Guidelines for the management of IT Security – Part 2: Managing and planning IT Security

[73] ISO/IEC TR 13335-3:1998 Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security

[74] ISO/IEC TR 13335-4:2000 Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards

[75] ISO/IEC TR 13335-5:2001 Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security

[76] KASSAI Károly: A magyar honvédség információvédelmének – mint a biztonság részének – feladatrendszere, doktori (PhD) értekezés (tervezet), Budapest, ZMNE, 2007 július 10.

[77] KOVÁCS László: Kritikus Információs Infrastruktúrák (egyetemi jegyzet), ZMNE, Budapest, 2007. – tervezet

[78] Lord JOPLING: The Protection of Critical Infrastructures, 036 CDS 07 E, Special report, 2007 tavaszi ülés, http://www.nato-pa.int/Default.asp?SHORTCUT=1165

[79] Magyar Értelmező Kéziszótár, Akadémiai Kiadó, Budapest, 1978./2003.

[80] Magyar Larousse Enciklopédikus szótár, Akadémiai Kiadó, Budapest, 1992.

[81] MARX György: Kockázat. In. Fizikai Szemle XL. évf. 1990. május p.129

[82] Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 12. számú ajánlása – BODLAKI Ákos-CSERNAY Andor-MÁTYÁS Péter-MUHA Lajos-PAPP György-VADÁSZ Dezső: *Informatikai Rendszerek Biztonsági Követelményei* – Budapest, 1996.

[83] Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 8. számú ajánlása – *Informatikai biztonsági módszertani kézikönyv* – Budapest, 1994.

[84] MSZ ISO 2382-1:1994 Információtechnika. Fogalommeghatározások. 1. rész: Alapfogalmak

[85] MUHA Lajos (szerk.): Az informatikai biztonság kézikönyve – Budapest: Verlag Dashöfer, 2000-2005.

[86] MUHA Lajos: Magyar Informatikai Biztonsági Irányítási Keretrendszer – Információs Társadalom Koordinációs Tárcaközi Bizottság Informatikai Biztonsági Albizottsága ülésen elhangzott előadás, Budapest 2005. 02. 28.

[87] National Information Assurance Strategy honlapja. http://www.cesg.gov.uk/

[88] OECD: Overwiew OECD Gudlines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD, 2002.

[89] POSTON, T.- STEWART, J.: Katasztrófaelmélet és alkalmazásai

[90] Prágai nyilatkozat, Észak-atlanti Tanács (állam- és kormányfők), 2002. november 21., Prága, http://www.nato.int/docu/0211prague/after_prague.pdf

[91] PRÉCSÉNYI Zoltán-SOLYMOSI József: Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé, Hadmérnök II. Évfolyam 1. szám – 2007. március, http://zrinyi.zmne.hu/hadmernok/archivum/2007/1/2007_1_precsenyi.html

[92] Proposal for a Regulation of the European Parliament and of the Council establishing the European Network and Information Security Agency, Euroai Bizottság, COM(2003)63, 2003.2.11.

[93] RÉNYI Alfréd: Valószínűségszámítás. Tankönyvkiadó, Budapest, 1954.

[94] SCHUMER, Chuk szenátor beszéde az Amerikai Egyesült Államok Szenátusa Jogi Bizottságának a kiberterrorizmus fenyegetésével foglalkozó ülésén, Wasington DC, 2002.02.13., http://www.senate.gov/~schumer/SchumerWebsite/pressroom/press_releases/PR00844.html

[95] Security within the North Atlantic Treaty Organisation (NATO) – C-M(2002)49

[96] SUTER, Manuel: A Generic National Framework For Critical Information Infrastructure Protection (CIIP), 2nd Facilitation Meeting for WSIS Action Line C5 háttéranyag, 2007. augusztus, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

[97] SZENES Zoltán: Válaszúton a a magyar biztonságpolitika. In: Új Honvédségi Szemle, 2005/12., online változat

[98] The National Strategy to Secure Cyberspace, Washington, White House, 2003. február

[99] US Patriot Act, 1016(e) Public Law 107-56 (42 U.S.C. 5195c(e))

[100] Zöld Könyv a kritikus infrastruktúrák védelem európai programjáról. (Előterjesztette a Bizottság). Európai Közösségek Bizottsága, Brüsszel, 2005. 11. 17. COM(2005)576 final, http://eur-lex.europa.eu/LexUriServ/site/hu/com/2005/com2005_0576hu01.pdf

[101] ZSIGMOND Gyula: Információs rendszerek energiaellátásának kérdései In. Informatika, Gábor Dénes Főiskola, Budapest, 2005. december, 8. évf. 4. sz. – p.78-81.

PUBLIKÁCIÓS LISTA

KÖNYV, JEGYZET

1. MUHA Lajos: *Magyar Informatikai Biztonság Irányítási Keretrendszer* – Információs Társadalom Koordinációs Tárcaközi Bizottság ajánlástervezet (http://www.itktb.hu/Resource.aspx?ResourceID=docstorefile&f=871&t=stored), Budapest, 2005. – 16p.
2. DÉRI Zoltán, LOBOGÓS Katalin, MUHA Lajos, NYÍRY Géza, SNEÉ Péter, VÁNCSA Julianna: *Az Informatikai Biztonság Irányításának Vizsgálata* (szerkesztő: Muha Lajos) – Információs Társadalom Koordinációs Tárcaközi Bizottság ajánlástervezet (http://www.itktb.hu/Resource.aspx?ResourceID=docstorefile&f=834&t=stored), Budapest, 2005. – 313p.
3. DÉRI Zoltán, LOBOGÓS Katalin, MUHA Lajos, SNEÉ Péter, VÁNCSA Julianna: *Az informatikai biztonság irányításának követelményrendszere* (szerkesztő: Muha Lajos) – Információs Társadalom Koordinációs Tárcaközi Bizottság ajánlástervezet (http://www.itktb.hu/Resource.aspx?ResourceID=docstorefile&f=833&t=stored), Budapest, 2004. – 207p.
4. MUHA Lajos - BODLAKI Ákos: *Az informatikai biztonság (egyetemi, főiskolai jegyzet)* – Budapest: PRO-SEC Kft. 2001. – 176p. – ISBN 963 86022 6 0
5. BODLAKI Ákos, MUHA Lajos: *Az informatikai biztonság tanúsítási és minősítési eljárásrendjének terve* – tanulmány a Miniszterelnöki Hivatal Informatikai Koordinációs Iroda részére, Budapest, 1997. – 112p.
6. BODLAKI Ákos, CSERNAY Andor, MÁTYÁS Péter, MUHA Lajos, PAPP György, VADÁSZ Dezső: *Informatikai Rendszerek Biztonsági Követelményei (Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság 12. számú ajánlás)*, Budapest: Miniszterelnöki Hivatal 1996. – 217p.
7. MUHA Lajos: *Adatvédelmi Jogszabálygyűjtemény* – FIXX Kft., Budapest: 1993 / Miniszterelnöki Hivatal *(a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság 8. számú ajánlás 5. számú mellékleteként)* 1995. – 213p.

SZERKESZTETT KÖNYVBEN CIKK

1. MUHA Lajos: *A szabályozási környezet által támasztott igények*, 6. fejezet In. SZIGETI Szabolcs, KRASZNAY Csaba, KREMSER Csaba, MUHA Lajos, RIGÓ Ernő: Útmutató az informatikai biztonság megvalósítására önkormányzatok számára (szerk. Szigeti Szabolcs) – Informatikai és Hírközlési Minisztérium ajánlása, Budapest, 2006. (http://www.itktb.hu/resource.aspx?ResourceID=it_bizt_onkormanyzatoknak_v1_0_rev_d_e_V1.doc) – p.104-109.
2. MUHA Lajos: *Az önkormányzati környezet specialitásai*, 7. fejezet In. SZIGETI Sz. et al.: Útmutató az informatikai biztonság megvalósítására önkormányzatok számára – Budapest, 2006. – p.110-112.

3. MUHA Lajos: *Jogszabályok*, 11. fejezet In. SZIGETI Sz. et al.: Útmutató az informatikai biztonság megvalósítására önkormányzatok számára – Budapest, 2006. – p.132-134.
4. MUHA Lajos: *Jogszabályok* – 1. kötet 2.2. pont In. Az informatikai biztonság kézikönyve (szerk. Muha Lajos) – Budapest: Verlag Dashöfer, 2000-2005 – ISBN 963 9313 12 2, 2000. november - 2005. március (többször frissítve)
5. MUHA Lajos: *Szabványok és ajánlások* – 1. kötet 2.3. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november - 2005. március (többször frissítve)
6. MUHA Lajos: *Fogalmak és definíciók* – 1. kötet 2.4. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2003. március, 2004. szeptember (frissítve)
7. MUHA Lajos: *Az informatikai biztonság kialakulása* – 1. kötet 3.2. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november, 2004. szeptember (frissítve)
8. MUHA Lajos: *Az informatikai biztonság meghatározása* – 1. kötet 3.3. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november, 2001. december, 2004. november (frissítve)
9. MUHA Lajos: *Az informatikai biztonság jogi szabályozása* – 1. kötet 3.4.1-3.4.6. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november, 2002. március (frissítve)
10. MUHA Lajos: *A számítógépes bűnözés* – 1. kötet 3.4.7. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november - 2005. március (többször frissítve)
11. MUHA Lajos: *ISO/IEC 17799:2000* – 1. kötet 3.5.1.6.1. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2001. szeptember
12. MUHA Lajos: *Az Informatikai Biztonság Irányításának Követelményrendszere* – 1. kötet 3.5.1.8. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2004. szeptember
13. MUHA Lajos: *Az informatikai biztonság irányításának vizsgálata és a tanúsítás eljárásrendje* – 1. kötet 3.5.1.9. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2004. szeptember
14. MUHA Lajos: *A Common Criteria* – 1. kötet 3.5.3.4. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2003. június
15. MUHA Lajos: *A titokvédelem és az Uniós csatlakozás* – 1. kötet 3.5.3.5. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2003. június
16. MUHA Lajos: *Az informatikai biztonsági hatóság* – 1. kötet 3.5.3.6. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2003. június
17. MUHA Lajos: *A titokvédelmi és az ügyviteli szabályzat* – 2. kötet 5.4.4. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november
18. MUHA Lajos: *Dokumentumkezelés, ügyvitel* – 2. kötet 5.7. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november, 2004. szeptember (frissítve)
19. MUHA Lajos: *Informatikai rendszerek biztonsági ellenőrzése* – 2. kötet 5.9.1. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november, 2001. szeptember (frissítve)
20. MUHA Lajos: *Az informatikai biztonsági vizsgálatot végző szervezetekkel és személyekkel szembeni követelmények* – 2. kötet 5.9.3. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2005. március

21. BODLAKI Ákos, ENDRÉDI Gábor, MUHA Lajos: *Tanúsított termékek* – 2. kötet 5.10. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november-2005. március (többször frissítve)
22. MUHA Lajos: *Az Informatikai Biztonság Irányítási Rendszer* – 2. kötet 5.12. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2005. június
23. HAJNAL János, MUHA Lajos: *Az informatikai rendszerek vállalkozásba adása* – 2. kötet 6.8. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november, 2005. június (frissítve)
24. MUHA Lajos: *Informatikai Biztonsági Szabályzat (ajánlás)* – 3. kötet 8.5. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2002. szeptember
25. MUHA Lajos: *A BS7799-2 szerinti audit* – 3. kötet 8.8. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2005. június

LEKTORÁLT FOLYÓIRATBAN MEGJELENT CIKKEK

1. MUHA Lajos: *Security Risk Analysis in ICT systems* In. Hadmérnök, ZMNE, Budapest, 2007. december
2. MUHA Lajos: *Az informatikai biztonság kérdései a felsőoktatásban* In. Informatika, Gábor Dénes Főiskola, Budapest, 2005. december, 8. évf. 4. sz. – p.96-99.
3. MUHA Lajos: *Az informatikai biztonság átértékelődött jelentősége napjainkban* In. Informatika, Gábor Dénes Főiskola, Budapest,, Budapest, 2005. december, 8. évf. 4. sz. – p.135-137.

KONFERENCIA KIADVÁNYBAN MEGJELENT ELŐADÁS

1. MUHA Lajos: *Az informatikai biztonság oktatása*, Felsőoktatási Matematika-, Fizika- és Számítástechnika Oktatók XXXI. Konferenciája, Dunaújváros, 2007.08.24. –p.202-205.
2. MUHA Lajos: *Informatikai biztonsági szabványok és irányelvek (a nemzetközi és a hazai szabályozás helyzete)*, IX. Országos Neumann Kongresszus, Győr, 2006.06.27. – CD mellékleten 10p.
3. MUHA Lajos: *A terrorizmus és az informatikai biztonság,* HiSec 2004 konferencia, Budapest, 2004.10.26.
4. Muha Lajos: *Szabványok és ajánlások az informatikai biztonság területén*, VIII. Országos Neumann Kongresszus, Budapest, 2003.10.17.
5. MUHA Lajos: *Az informatikai biztonság felügyeleti és tanúsító intézményrendszere,* HiSec 2003 konferencia, Budapest, 2003.10.29.
6. MUHA Lajos: *Az informatikai biztonság*, EDI ’98 konferencia, Budapest, 1998.07.18.
7. MUHA Lajos: *Az elektronikus okirat bevezetésének kérdései ...*, HiSec ’97 konferencia, Budapest, 1997.06.06.
8. MUHA Lajos: *Az informatikai biztonság auditálása*, HiSec ’96 konferencia, Budapest, 1996.06.14.

RÖVIDÍTÉSEK JEGYZÉKE

rövidítés	angol (eredeti)	magyar
ATM	Automatic Teller Machine	bankjegykiadó automata
BSI	British Standard Institute	Brit Szabványügyi Hivatal
CAPC	Civil Aviation Planning Committee	Polgári Repülés Tervező Bizottság
CC	Common Criteria	Közös Követelmények
CCPC	Civil Communication Planning Committee	Civil Kommunikáció Tervező Bizottság
CCTA	Central Computer and Telecommunications Agency	Központi Számítógép és Távközlési Ügynökség
CCU	Computer Crime Unit	Számítógépes Bűnügyi Egység
CEP	Civil Emergency Planning	Polgári Vészhelyzeti Tervezés
CERT	Computer Emergency Response Team	Számítógépes Vészhelyzeti Reagáló Csoport
CI2RCO	Critical Information Infrastructure Research Co-ordination	Kritikus Információs Infrastruktúrák Fejlesztési Koordináció
CIIP	Critical Information Infrastructure Protection	kritikus információs infrastruktúrák védelme
CIP	Critical Infrastructure Protection	kritikus infrastruktúrák védelme
CIWIN	Critical Infrastructure Warning Information Network	Kritikus Infrastruktúra Figyelmeztető Információs Hálózat
CNI	Critical National Infrastructure	kritikus nemzeti infrastruktúra
COBIT	Control Objectives for Information and Related Technology	Informatika Irányítási és Ellenőrzési Módszertan
CPC	Civil Protection Committee	Polgári Védelmi Bizottság
CRAMM	CCTA Risk Analysis and Management Method	CCTA Kockázatelemzési és Kezelési Módszertan
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria	Kanadai Biztonságos Számítástechnikai Termékek Értékelési Kritériumok
CSIRT	Computer Security Incident Response Team	Számítógépes Biztonsági Incidens Reagáló Csoport
CSTARC	Cyber Security Tracking, Analysis and Response Center	Hálózatbiztonsági Követő, Elemző és Reagáló Központ
DDoS	Distributed Denial of Service	szolgáltatás megtagadás
DDSI	Dependability Development Support Initiative	Megbízható Fejlődést Támogató Kezdeményezés
DG INFSO	Directorate-General for Information Society and Media	Információs Társadalom és Média Főigazgatóság
DHS	Department of Homeland Security	Belbiztonsági Minisztérium
DSTL	Defense Science and Technology Laboratory	Védelmi Tudományos és Technológiai Laboratórium
ECI	European Critical Infrastructure	európai kritikus infrastruktúra
EGC	European Governmental CERTs	Európai Kormányzati CERT-ek
ENISA	European Network and Information Security Agency	Európai Hálózat- és Informatikai Biztonsági Ügynökség
EPCIP	European Programme for Critical Infrastructure Protection	Európai Kritikus Infrastruktúra Védelmi Program
EU	European Union	Európai Unió
FAPC	Food and Agriculture Planning Committee	Élelmiszer és Agrár Tervező Bizottság
FC	Federal Criteria for Information Technology Security	Szövetségi Információtechnológiai Biztonsági Kritériumok

rövidítés	angol (eredeti)	magyar
FIRST	Forum of Incident Response Teams	Eseménykezelő Csoportok Fóruma
GAKI	German Arbeitsgruppe Kritischer Infrastructuren	Német Kritikus Infrastruktúra Munkacsoport
HSDP	Homeland Security Presidential Directive	Belbiztonsági Elnöki Iránymutatás
ICT	Information and Communications Technology	információs és kommunikációs technológiák
IEC	International Electrotechnical Commission	Nemzetközi Elektrotechnikai Bizottság
IKT	Information and Communications Technology	információs és kommunikációs technológiák
INFOSEC	information security	elektronikus dokumentumvédelem
IPC	Industrial Planning Committee	Ipari Tervező Bizottság
ISAC	Information Sharing and Analysis Centre	Információ Elosztó és Elemző Központ
ISACA	Information Systems Audit and Control Association	Informatikai Rendszer Ellenőrök Egyesülete
ISMS	Information Security Management Systems	Informatikai Biztonsági Irányítási Rendszerek
ISO	International Organization for Standardization	Nemzetközi Szabványügyi Szervezet
IST	Information Society Technologies	Információs Társadalom Technológiái
ITB	Interministerial Committee on Information Technology	Informatikai Tárcaközi Bizottság
ITIL	Information Technology Infrastructure Library	Informatika Szolgáltatás Módszertan
ITKTB	Interministerial Committee on Information Society	Információs Társadalom Koordinációs Tárcaközi Bizottság
IWWN	International Watch and Warning Network	Nemzetközi Figyelmeztető és Jelző Hálózat
MeH	Prime Minister's Office	Miniszterelnöki Hivatal
NATO	North Atlantic Treaty Organization	Észak-atlanti Szerződés Szervezete
NCSD	National Cyber Security Division	Nemzeti Hálózatbiztonsági Főigazgatóság
NHTCU	National High Technology Crime Unit	Nemzeti Fejlett Technológiai Bűnüldözési Egység
NISCC	National Infrastructure Security Coordination Centre	Nemzeti Infrastruktúra Biztonsági Koordinációs Központ
NIST	National Institute of Standards and Technology	Nemzeti Szabványügyi és Technológiai Intézet
OCLCTIC	Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication	Információs és Kommunikációs Technológiákhoz Kötődő Bűnözés Elleni Harc Központi Hivatal
PB&Cs	Planning Boards and Committees	Tervező Csoportok és Bizottságok
PBIST	Planning Board for Inland Surface Transportation	Közúti Szállítások Tervező Csoport
PBOS	Planning Board for Ocean Shipping	Tengeri Hajózás Tervező Csoport
PDA	Personal Digital Assistant	digitális személyi asszisztens
PKI	public key infrastructure	nyilvános kulcsú infrastruktúra
PPP	Public Private Partnership	állami-magán társulás
SCADA	Supervisory Control and Data Acquisition	felügyelet-irányítás és adatgyűjtés
SCEPC	Senior Civil Emergency Planning Committee	Polgári Vészhelyzeti Tervező Bizottság
TCSEC	Trusted Computer System Evaluation Criteria	Biztonságos Számítógéprendszer Értékelési Követelmények
UNIRAS	Unified Incident Reporting and Alert Scheme	Egyesített Incidens Jelentő és Figyelmeztető Séma
WARP	Warning, Advice and Reporting Point	Figyelmeztető, Tanácsadó és Jelentő Pont
WTC	World Trade Center	Világkereskedelmi Központ

TÁBLÁZATOK JEGYZÉKE

ÁBRÁK JEGYZÉKE

EGYENLETEK JEGYZÉKE